SEGURIDAD EN SERVIDORES LINUX NOTA 3



$8,80 EN TODO EL PAIS

REVISTA DE NETWORKING Y PROGRAMACIÓN

#24

HARDWARE
Servidores Corporativos

SEGURIDAD
en dispositivos Móviles

E-LEARNING

STORAGE
CONSOLIDACIÓN - VIRTUALIZACIÓN
ADMINISTRACIÓN

EL NEGOCIO
Tendencias en desarrollo del Software: NOTA #1

Alta Disponibilidad en
SQL 2005

INNOVADORES IT



APRENDA CON LOS **MEJORES**

"Portal de Gestión Comercial en Java bajo Plataforma Linux"
Diego Marsili - Gerente de Sysbase Professional Services.


WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00024
Dist. Cap.: Vaccaro Sanchez y Cia. S.C. - Interior: DGP
Correo Argentino FRANQUEO A PAGAR Cta. 16185

NEX IT SPECIALIST #24

- STORAGE - CONSOLIDACIÓN, VIRTUALIZACIÓN Y ADMINISTRACIÓN -

DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

EDITORES
- Carlos Vaughn O'Connor
- Carlos Rodríguez

EDITOR TÉCNICO
- Alejandro Cynowicz
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
- Andrés Vázquez
- Martín Guaglianone
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. C1091AAP- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1 C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar





Nota del Editor

Paul Clark en su libro "Storage Virtualization" (Editado por: Addison-Wesley Professional, 2005) dice:
"La industria del almacenamiento de datos es hoy en día uno de los más dinámicos sectores en IT. Debido, en gran parte, a la introducción del networking de alta performance entre activos de storage y servidores, la tecnología de storage ha sufrido una rápida transformación mientras una innovación tras otra ha impulsado las soluciones de storage para adelante. Al mismo tiempo, la viabilidad de nuevas tecnologías de almacenamiento es afirmada repetidamente por la rápida adopción de storage en red por virtualmente cada empresa e instituciones de gran tamaño. Gobiernos, empresas, e instituciones dependen hoy de la información, y ésta, en forma de datos reside en última instancia en algún lugar en un medio de storage. Aplicar nuevas tecnologías para salvaguardar estos datos esenciales, facilitar su acceso, y simplificar su administración tiene un valor indiscutible

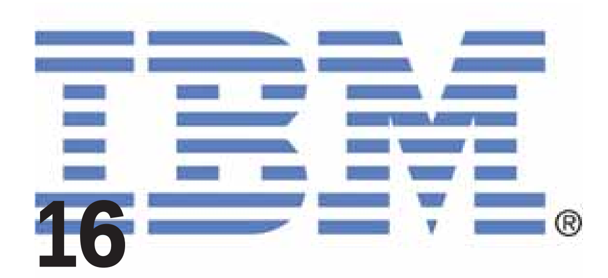
Desde comienzos de los noventas, las innovaciones en storage han producido un flujo constante de nuevas soluciones tecnológicas, incluyendo Fibre Channel, network-attached storage (NAS), clustering de servidores, serverless backup, dual-pathing de alta disponibilidad, copia de datos point-in-time (snapshots), acceso a cintas compartidas, storage a distancia, iSCSI, administración de activos de storage y transporte basados en CIM (common information model), y virtualización de storage. Cada una de estas sucesivas olas de avances tecnológicos han sido acompañadas por el abandono de viejas prácticas, sobrevaluación de lo que la nueva solución podría en realidad hacer, y confusión entre consumidores. En última instancia, sin embargo, cada paso en el desarrollo técnico eventualmente termina siendo de utilidad, y toda acción de marketing encuentra su lugar".

En NEX #24, aparecerán a lo largo de diferentes artículos escritos por los principales players, los siguientes conceptos/protocolos/algoritmos: NAS, SAN, VSAN, seguridad en storage, virtualización, autenticación, autorización, IPsec, FC-SP, AES, DES, 3DES para iSCSI, FCIP), SSL, SSHv2, TACAS, RADIUS, SNMPv3, GRID y otros. Si Ud. conoce sobre todos ellos puede saltear los artículos de storage en esta edición.
NEX se complementa con artículos individuales de temas variados del mundo IT o propuestos como una serie (Seguridad en servidores Linux, Tendencias en el desarrollo de software, Servers en PYMES y corporaciones). Como siempre los invitamos a escribirnos y darnos vuestra opinión a *redaccion@nexweb.com.ar*



Barrer la web para conocer su estructura de links requería una cantidad enorme de storage en comparación con las necesidades típicas para proyectos estudiantiles. Nada más interesante para arrancar con almacenamiento que conocer la computadora de storage original usada por Google en 1996 [ver Page y Brin en el museo de computación de Universidad de Stanford (http://www-db.stanford.edu/)]. Aquí vemos el arreglo original, que contenía 10 disk drives de 4GB cada uno, dando un total de 40GB.

SUMARIO



16

Evolución de los Sistemas de Storage

En este artículo se mostrará como los sistemas de storage han evolucionado en las últimas cinco décadas, siempre buscando satisfacer las necesidades de los clientes.



28

Optimizando su SAN

Las empresas deberían soportar las técnicas de aceleración de SAN, seguridad multifacética, y capacidades e interfaces de administración de estandarizadas industrialmente, para asegurar que su SAN se desempeñe bien y permanezca segura, con costos reducidos, y administrable.

TENDENCIAS DEL SOFTWARE



El Negocio del Sofrware y Servicios Informáticos



46

El objetivo de este artículo es presentar la experiencia vivida por los socios de un emprendimiento que consistió en montar una consultora de sistemas.

Seguriinfo 2006

El 15 de marzo se realizó SEGURINFO 2006. La segunda edición del Congreso Nacional de Seguridad de la Información, organizado por Usuaria (Asociación Argentina de Usuarios de la Informática y las Comunicaciones)



El evento tuvo lugar en el salón Retiro del Hotel Sheraton Buenos Aires y congregó a más de 1400 asistentes que participaron de las conferencias de expertos de las organizaciones más reconocidas del mercado en seguridad, duplicando la convocatoria del año anterior.

Algunos de los temas más importantes que se trataron durante el Congreso fueron:

- Realidad de Hoy, Estadísticas, Costos y Nueva Versión de Sarbanes Oxley
- Phishing y Pharming
- Análisis de Normas y Metodologías que Afectan a la Gestión de Seguridad de la Información
- Cómo Crear y Sustentar un Programa de "Awarness" en Seguridad.
- Convergencia en la Seguridad Empresarial
- Gerenciamiento de la Seguridad de Información
- ROSI, ROI de la Seguridad de la Información
- Fiabilidad de Sistemas y Equilibrios de Nash
- Bluetooth - Una Amenaza Creciente
- Biometría en Seguridad Lógica y Física
- Normativas ISO Gestión de Seguridad de la Información (Serie 27000, ex ISO 17799)
- Implementación Bs7799 - Caso Real
- Seguridad Legal: Habeas Data, Protección y Privacidad de Datos, Firma Digital, Factura digital
- Seguridad Forense: Peritajes, Fraudes Electrónicos y Análisis Forense Informático
- Seguridad Técnica: Accesos Externos y Protección de Datos, Nuevas Tecnologías para la Autenticación Remota de Usuarios
- Preservación Física y Lógica de Software (Escrow)





Oracle Day

El 16 de marzo se realizó el Oracle Open Day, en el marco del Fusion Roadshow Latin America. El evento se realizó en el Zanjón de Granados, monumento histórico en San Telmo, que albergó toda la oferta de soluciones de negocios de Oracle.

Las dos plantas del Zanjón de Granados (Salón de Los Patios y Salón del Pasaje) albergaron charlas sobre soluciones de Oracle, además de las presentaciones de sponsors y socios de negocios de la compañía.

Los sectores dedicados especialmente a los servicios de Consultoría, Soporte y Educación de Oracle recibieron gran afluencia de público, que presenció actividades específicas de cada área a cargo de especialistas, como Lifetime Support y Oracle University.

Sun Microsystems, Intel, EMC, HP, IT Convergence, Grupo Quanam, NetApp, Sofrecom, Grupo MOST, BGH, ICS, Red Hat, Minder S.A. y Open Solutions Argentina S.A., entre otros, ofrecieron también presentaciones individuales sobre su expertise y casos de éxito de implementaciones de Oracle.

ORACLE



CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2006

Fecha		Informes
	ABRIL	
20	**IDC IT Storage & InfrastructureVision Conference** Marriott Plaza Hotel, Buenos Aires	jbotter@idc.com www.idclatin.com/argentina
26	**IBM Software Day 2006 -** 8.30 hs. hotel Hilton Buenos Aires, Av. Macacha Güemes 351, Salón Pacífico, 2° Subsuelo, Puerto Madero, Capital Federal	http://www.ibm.com/ar/news/events/swday/index.phtml
	MAYO	
3	**Jornadas Trabajo IT -** Sheraton Buenos Aires	www.worktec.com.ar - info@worktec.com.ar
	JUNIO	
8	**Jornadas Trabajo IT Córdoba -** Córdoba Capital.	www.worktec.com.ar info@worktec.com.ar Tel.:4511.3300
9	**CIASFI Córdoba -** Córdoba Capital.	
22	**1er Jornada Nacional de Calidad en Software -** Sheraton Libertador.	
	SEPTIEMBRE	
19 y 20	**Consecri-Consetic 2006 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	OCTUBRE	
3 al 6	**EXPO COMM -** La Rural, Predio Ferial de Buenos Aires.	www.expocomm.com.ar
6 y 7	**2do Congreso Nacional de Estudiantes de Sistemas y Tecnología de la Información. -** Lugar a confirmar.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	NOVIEMBRE	
2	**Jornadas Trabajo IT 2 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar
2 al 5	**AES - Argentina Electronic Show -** La Rural, Predio Ferial de Buenos Aires.	http://www.aeshow.com.ar/es_services_contact_us

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar

Portal de Gestión Comercial en Java bajo plataforma Linux



En la actualidad los desarrollos WEB tienen otra dirección debido al avance tecnológico y a la necesidad de administrar vía Internet grandes volúmenes de datos. La palabra 'Performance' en estos proyectos es clave y ocupa el primer lugar de importancia. Surgen, también, nuevos requerimientos tales como: Integración, Publicación, Autenticación, Paginación, Persistencia, Caching, Scheduling...
Pero, ¿Cómo es una implementación real? ¿Qué involucra? ¿Sencilla, difícil, compleja? La respuesta: sencilla, si se tiene el conocimiento. El artículo describe todos los parámetros que se debieron tener en cuenta y todas las tecnologías que fueron necesarias dominar para la implementación del portal de la empresa del rubro inmobiliario L.J. Ramos.

Diego Marsili
Professional Services Manager - Sybase S.A.

Desafío

A comienzos del año 2004 realizamos una propuesta de servicios profesionales para un nuevo cliente. El rubro inmobiliario fue nuestro objetivo y la empresa L.J.Ramos nos abrió sus puertas. Las primeras etapas del proyecto fueron de vital importancia y nos encaminamos en la ardua tarea de tomar requerimientos funcionales. La colaboración fue inmediata pero nos dejaron entrever ciertos prejuicios a la hora de optar por tecnologías Web. Con el avance del proyecto y luego de documentar todas las tareas de relevamiento decidimos realizar un prototipo y fue así como comenzamos a delinear los componentes y las funciones del sistema. Desarrollamos cada una de las pantallas principales y en este marco definimos uno a uno los módulos a implementar (Agenda Comercial, Recepción o Mesa de Entrada, Gestión Comercial, Publicidad, Mailing, Administración Contable, Alarmas y Auditorías).

> ***Framework:*** *en el desarrollo de software, un framework es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, un framework puede incluir soporte de programas, librerías y un lenguaje de scripting entre otros software para ayudar a desarrollar y unir los diferentes componentes de un proyecto).*

Durante las reuniones con gerentes comerciales, usuarios y responsables de sistemas observamos que se efectuaban tareas cotidianas utilizando herramientas aisladas, la integración se realizaba de forma manual , y tenían necesidades de documentación, administración, gestión y control centralizado.
La implementación resultó muy interesante, teniendo que valernos de diferentes frameworks, asimismo podemos destacar que no es necesario repetir algo hecho, siempre que esté bien desarrollado.
A continuación enunciaré los requerimientos más relevantes y desafiantes que nos llevaron a investigar y desarrollar diversas soluciones:
- Personalización, integración y publicación de los sitios ya desarrollados para Intranet.
- Autenticación y administración de seguridad .
- Desacoplar el contexto de la interfaz grafica de la lógica del negocio.
- Scheduling (Alarmas por vencimientos de alquileres, contratos, pagos de comisiones, cierre de avisos publicitarios y eventos relacionados con la agenda comercial).
- Representación geográfica (georeferenciación) de propiedades y representación cartográfica superponiendo capas (bancos, hospitales, cajeros automáticos etc.).
- Buscador de propiedades vecinas vigentes.
- Generación de reportes en diferentes formatos a partir de adjuntos, fotos y mapas.
- Integración con el correo electrónico.
- Acceso desde Internet e Intranet a los usuarios finales.
- Performance, Paginado y Técnicas de Cache.
- Actualización Automática de novedades e imágenes en el buscador de propiedades de acceso público (disponibilidad 7 X 24), con hosting externo, desarrollado con tecnología .NET.

Implementación

Les aclaro, que para mantener el compromiso de confidencialidad y por normas de seguridad, omitiré las versiones de los productos. La plataforma elegida para todos ellos es Red Hat Enterprise. Y los productos participantes en la solución son: Sybase Enterprise Portal Information Edition, Sun One Directory Server y el DBMS es Sybase Adaptive Server Enterprise.
- *Personalización, integración y publicación:* este requerimiento fue resuelto utilizando "Sybase Enterprise Portal Information Edition" (release compilado para Linux basando su contenedor Servlet/JSP en Tomcat). Este producto nos permitió integrarnos con las aplicaciones desarrolladas para la Intranet desde diferentes portlets supervisados y publicados hacia los diferentes roles del árbol organizacional.
Los portlets pueden ser construidos partiendo de diferentes fuentes o capturando contenido proveniente de diversas tecnologías: HTML, JSP, ASP, XML, SQL, Documentos y WebServices.



LDAP: Lighweight Directory Access Protocol, es un protocolo de red que permite el acceso a un servicio de directorio ordenado y distribuido. Almacena información de login, certificados, permisos etc.)

usualmente una interfaz y el Controlador responderá a los eventos (ver Figura1). Como implementación a este patrón aparecieron varios frameworks, en nuestro caso optamos por utilizar Struts y la razón fue principalmente la aceptación del mercado en los últimos años. Sin dudas este patrón se presenta para disminuir la complejidad en el desarrollo de aplicaciones web.

- Scheduling: la funcionalidad de programación de alarmas y eventos se incrementó muchísimo porque en un principio estaba orientada a algunos casos aislados, como recordatorio de vencimientos de contratos de exclusividad, liquidaciones por diferentes conceptos, avisos por cierre cercanos a fechas de publicación, retiro de carteles en una propiedad etc. Cada vez eran más los motivos y fue en ese entonces que decidimos desarrollar un módulo de alarmas y eventos genérico con posibilidad de reprogramaciones agregando también la posibilidad de otorgar prioridades. Resumiendo aspectos de la implementación utilizamos un framework de la firma OpenSymphony denominado Quartz que nos permite schedulear trabajos en entornos Java. Los trabajos pueden ser componentes estándares Java o EJB. Puede ser instanciado como un cluster con capacidad de balanceo de carga y soporte a fallas. (Ejemplo 1)

- Representación geográfica de propiedades y representación cartográfica: utilizamos un ActiveX de la firma Cybermapa, el cual fue integrado a nuestra solución. Así se logró representar cartográficamente la latitud y longitud de cada propiedad con características de zoom in, zoom out, capas (bancos, hospitales, cajeros, etc.), búsqueda de direcciones, apertura de fichas de propiedades partiendo de un punto del mapa etc. En cuanto a la generación de las vistas de los mapas incluidos en los informes y reportes desarrollamos un clien-

La personalización estará dada por la posibilidad que posee el usuario final de administrar la presentación gráfica de páginas y portlets dependiendo de su utilización. Ésto le permitirá publicar contenidos, novedades y generar paneles de control hacia diferentes unidades de negocio dentro de la organización.

- *Autenticación y administración de seguridad:* este es un tema muchas veces complejo en algunas organizaciones y agravado por las implementaciones multiplataforma, por ello utilizamos un directorio común con soporte a aplicaciones de diferentes plataformas y sin la necesidad de implementar una solución basada en un DBMS. Por tal motivo seleccionamos para nuestra implementación Sun One Directory Server para Linux. Desde el Portal nos integramos con este LDAP Para otras implementaciones (Active Directory, Open LDAP, IPlanet) utilizamos un conector, tipo Realm para Tomcat, el cual otorgó al Portal la posibilidad de autenticar y delegar todos los temas relacionados a la administración de seguridad de la organización (múltiples sucursales, unidades de negocio, usuarios, roles etc.).

El acceso hacia el LDAP desde los diferentes servicios JAVA se realizó por vías estándares de acceso JNDI y a través de diferentes controles de búsqueda.

- Desacoplar el contexto de la interfaz grafica de la lógica del negocio: nos basamos en las arquitecturas para JSP conocidas como Modelo 2. Esta arquitectura presenta un patrón de Modelo, Vista y Presentación (MVC) donde el Modelo es la representación especifica del dominio de la información, la Vista presentará al modelo en un formato,

Portlet: es un componente java administrado por un contenedor que procesa requests y genera contenido dinámico. Los portales utilizan portlets como un recurso para brindar componentes de interfaz de usuario a sistemas de información. Existe una especificación de portlets denominada JSR168, se puede consultar en (http://www.jcp.org/en/ jsr/detail?id=168)

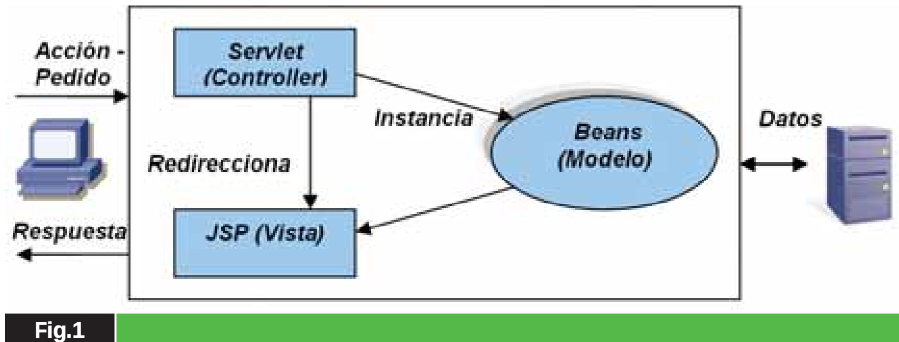


Fig.1

```
JobDetail jobDetail = new JobDetail("myJob",//job name
sched.DEFAULT_GROUP,CustomJob.class);//clase java a ejecutar

  Trigger trigger = TriggerUtils.makeDailyTrigger(8, 30);
  trigger.setStartTime(new Date());
  trigger.setName("myTrigger");
  sched.scheduleJob(jobDetail, trigger);
```

Ej.1 Ejemplo de un Job utilizando Quartz

JNDI API: *es un estándar para acceder y nominar directorios. El JNDI API tiene dos partes: una interfase de nivel de aplicación usada por los componentes de la aplicación para acceder al servicio de nombres y directorios, y un servicio del proveedor para enlazar nombres y directorios)*

te http para realizar llamadas desde Java al mapserver (webserver de mapas en plataforma NT) mapeando algunos recursos externos con Samba.

- Generación de Informes y Reportes: para la generación de reportes de gestión con posibilidades de exportación a diferentes formatos (PDF, Excel, HTML, XLS, CSV, XML) utilizamos una herramienta OpenSource de tipo WYSIWYG diseñada para JasperReport llamada IReport (Ver Figura 2) (Pastilla-JasperReport: es una herramienta OpenSource, escrita en Java, para generación de reportes en diferentes formatos que pueden ser direccionados hacia una impresora y utilizados en aplicaciones Java, incluidas J2EE y Web). IReport es una GUI que permite generar los archivos de definición (en XML), compilarlos y previsualizar las diferentes posibilidades de exportación. Otras herramientas GUI que se pueden utilizar en la definición de los reportes son: JasperAssitant, JasperPal, JasperReportViewer plugin for Jedit, OpenReports Designer, SWTJasperViewer
- Integración con el correo electrónico: nos integramos a Novell Groupwise utilizando el estándar JavaMail, permitiendo enviar correo desde el Portal integrando los módulos de agenda, informes, cartografía, mailing, auditoría y gestión comercial al correo electrónico en cada uno de los puestos de trabajo.
- Performance, Paginado y Técnicas de Cache: la velocidad de respuesta fue un factor clave para la aceptación de la solución. Con varios desarrollos de Portales en nuestro haber, tratamos de aprovechar al máximo todos los aspectos que en conjunto permitieron que la aplicación funcione en los tiempos de respuesta pedidos. En cuanto a la distribución de la presentación utilizamos diferentes frames para asegurarnos de que solamente el contenido dinámico sea el refrescado. Limitamos la cantidad de registros a visualizar en las tablas html por medio de técnicas de paginado, existen varios frameworks que codificando muy poco nos permiten obtener estos resultados, les recomiendo probar *displaytag*. La velocidad de respuesta de los servicios java se vio favorecida por la ejecución de stored procedures en Adaptive Server Enterprise accediendo únicamente por claves tipo identity y evitando el uso de cláusulas join.

Todas las tablas descriptivas (código, descripción) se cargan previamente en componentes java que las mantienen en memoria conformando un único cache o espacio temporal y se refrescan por demanda dependiendo de las acciones de actualización sobre la base de datos. Por último, no debemos olvidarnos de las configuraciones adicionales sobre Apache Web Server. La cantidad de elementos solicitados desde un browser y la cantidad de objetos innecesarios que viajan cada vez que se carga una página es un tema que a mi criterio despierta poco interés y es donde realmente se obtienen resultados inmediatos sin necesidad de innovar en hardware.

Volviendo a Apache pueden agregar un módulo denominado mod_expires, por medio de la instrucción "LoadModule expires_module modules/mod_expires.so", el cual genera un encabezado "HTTP Expires" de acuerdo a criterios de configuración del servidor.

Por si no fui claro, luego de agregar este módulo puedo configurar directivas del tipo "ExpiresByType image/gif A2592000" para que los elementos de tipo gif expiren luego de un mes en el cache del cliente. En nuestra solución imputamos una fecha de expiración a los archivos de hojas de estilo, javascript e imágenes para que no realicen viajes innecesarios.

- Actualización automática de imágenes y novedades en un buscador de dominio público: uno de los objetivos principales de la solución era tener una única base de datos centralizada que pueda brindar servicios a sitios hosteados con respuesta de tipo 7x24 (siete días a la semana las 24 horas). El cliente ya contaba con un sitio pensado como buscador de propiedades, desarrollado en .NET y necesitábamos dar soporte a procesos que actualicen las novedades periódicamente. La solución llego del lado de los WebServices y con la implementación de SOAP ("Simple Object Access Protocol") de Apache conocida como AXIS. SOAP es un protocolo de intercambio de información , está basado en XML y estandarizado por el consorcio W3C.

Sin mucho esfuerzo agregamos a las clases de nuestros servicios la posibilidad de transformar objetos en XML. Como siempre existen muchos frameworks y en este caso nos inclinamos por *xstream*. A través de él serializamos objetos a XML. (Ej.2)

Samba: *es un software open source que brinda la posibilidad de acceder a archivos y servicios de impresión de clientes Windows, también recomiendo Sharity-Light que es muy fácil de compilar para Unix y muy conocido por la gente de Mac OS X)*

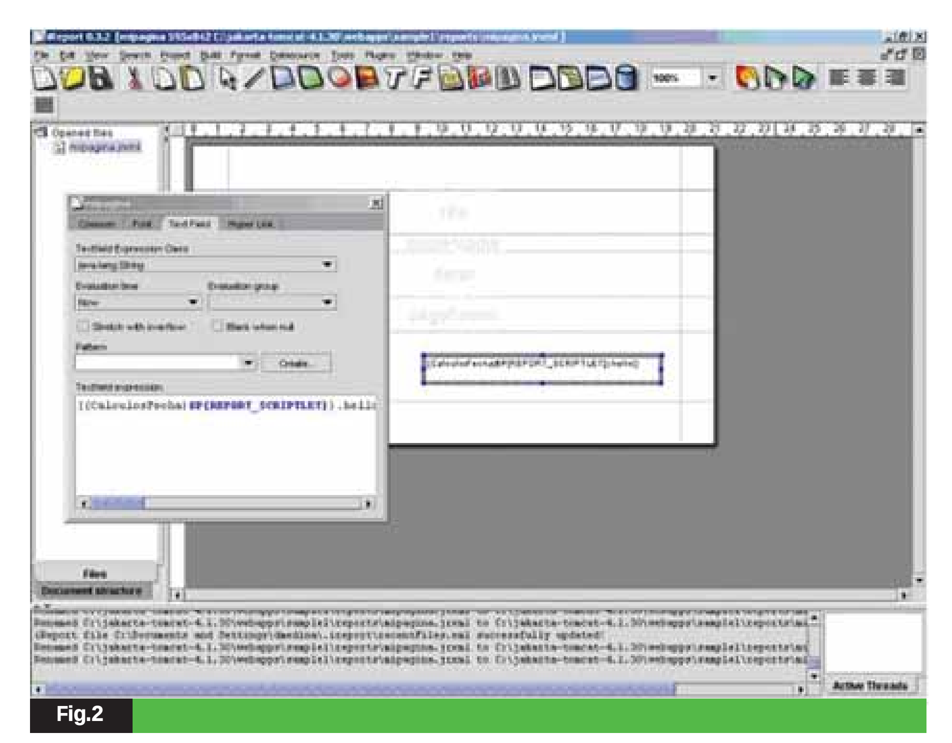


Fig.2

Sitios de Interés:

http://xstream.codehaus.org/
http://ws.apache.org/axis/
http://www.theserverside.com/tss
http://struts.apache.org/
http://www.sybase.com/
http://jasperreports.sourceforge.net/
http://displaytag.sourceforge.net
http://java-source.net/
http://www.opensymphony.com/quartz/
http://jakarta.apache.org

```
import com.thoughtworks.xstream.XStream;

public class Usuario {
          private String nombre;
          private String apellido;
          public Usuario(String nombre, String apellido) {
                    this.nombre = nombre;
                    this.apellido = apellido;
          }
          public static void main(String[] args) {
                    XStream xstream = new XStream();
                    Usuario usu = new Usuario("Raul","Perez");
                    xstream.alias("Usuario", Usurio.class);
                    String xml = xstream.toXML(usu);
                    System.out.println(xml);
          }
}
Salida
<Usuario>
  <nombre>Raul</nombre>
  <apellido>Perez</apellido>
</Usuario>
```

Ej.2 Ejemplo XStream



El daño colateral de sus errores

David Alejandro Yanover
Director de www.MasterMagazine.info

Cientos de sitios de Internet perdieron más del 70% de sus visitas durante un largo período de tiempo a partir de un error interno de Google, que provocó que estas páginas desaparecieran de las primeras listas de resultados.

Un error en el proceso de indexación de Google, que captura las distintas páginas de Internet para luego presentarlas en un orden de prioridad ante una determinada consulta de búsqueda, originó un huracán que arrasó con cientos de sitios Web, muchos de los cuales eran conocidos por mantener una sólida y destacada presencia en Internet.
La problemática que en los primeros días de marzo hizo estallar las comunidades sobre desarrollo y promoción Web no era nueva, pero su efecto se expandió y nuevas páginas fueron afectadas. En este artículo no sólo analizamos el hasta ahora mayor problema técnico de Google en lo que va del año, sino que al mismo tiempo se reflejará el papel dominante del buscador sobre la Internet actual. Hoy en día, para muchas personas, Google es Internet.
El error fue incluso aceptado como tal desde Google, según dejó trascender el 8 de marzo "GoogleGuy", un ingeniero del buscador que detrás de su Nick tiene contacto con desarrolladores de sitios a partir de apariciones en foros de debate, como los que se dan en WebmasterWorld.com. Otro nombre clave que hace de puente entre Google y los dueños de páginas es Matt Cutts, que tiene su propio blog en www.mattcutts.com/blog. Para los curiosos, muchos creen que "GoogleGuy" y Matt Cutt son la misma persona.
En aquél momento, "GoogleGuy" informó que estaban trabajando en una solución ante el problema advertido por numerosos webmasters, y que una semana después se estaría resolviendo. En efecto, fue así. Sin embargo, al día de hoy muchos sitios continúan pagando el error de Google, mientras que otros rezan por no volver a caer luego de haber soportado difíciles situaciones económicas.
El interrogante de si uno puede confiarle su negocio online a Google es uno de los planteamientos a los que se responderá en este artículo, porque este grave problema que aún padece Google (pero que fue solucionado en gran parte) ha puesto en evidencia su papel sobre el futuro de cualquier proyecto de Internet. Porque Google, además de ser una empresa privada que cuida sus intereses, tiene una repercusión sobre todos los sitios, debido a su incesante demanda.

El síntoma de la enfermedad de las Páginas Suplementarias

Todos los sitios afectados mostraban como característica el hecho de que cada una de las páginas internas del sitio, a excepción del dominio principal, eran marcadas como "Resultados Suplementarios". Para identificar el estado de una Web, la consulta site:www.midominio.com en Google proporciona la respuesta.
Que una página sea considerada como "Resultado Suplementario" implica que su valor dentro del índice de resultados es mucho más pobre que el del resto, porque la misma está precisamente en proceso de análisis de indexación. Una página suplementaria es usualmente una URL que fue recientemente eliminada. Por lo tanto, que un sitio de años de vida en Internet vea convertidas a este estado el 99.9% de sus contenidos, es un serio error.
¿Es ésto algún tipo de penalización? Muchos lo han confundido con una respuesta de Google ante acciones que van en contra de sus criterios de "información útil para el navegante", porque de hecho Google efectivamente es cada vez más riguroso al analizar los contenidos de los sitios de la red. Los filtros de información duplicada que penalizan cuando un sitio roba contenidos de otro de forma masiva, o el efecto Sandbox que afecta a dominios nuevos y da poder a URL's de años de presencia en la Web, son sólo dos criterios de revi-

Keyword Density - SEO Tools - Search Engine Optimization, Google ... - [Traduzca esta página]
Receive suggestions for popular key-terms related to your current ones, from the SEO Chat Keyword Suggestion tool.
www.seochat.com/seo-tools/keyword-density/ - 77k - Resultado Suplementario
En caché - Páginas similares

sión de una lista que solamente Google sabe donde termina. Esta problemática afectó a sitios sin ningún tipo de discriminación, lo cual dio lugar a todo tipo de hipótesis en las comunidades dedicadas al Posicionamiento Web, acerca de por qué se dio esta situación.
El problema fue propio de Google, y para que un sitio regresase a su estado normal, lo único que podía hacer era esperar... no es raro que surjan pequeños incidentes en Google o en otro buscador, pero en esta oportunidad no se trató de un problema menor.
Y los propios navegantes también recibieron el daño colateral, ya que los resultados a sus búsquedas eran de menor relevancia. Pero, por suerte para Google, este grupo es el que menor percepción tuvo del error, como suele suceder.

El caso de Musica24.NET

La forma más directa de comunicar y analizar un hecho de estas características, es a partir de casos concretos, de tal manera de apreciar los daños reales. En esta ocasión, vemos lo que sucedió con el sitio www.musica24.net, del cual se tuvo acceso a su información estadística. Musica24.net es un espacio en el que se analiza la actualidad del ambiente de la industria discográfica y sus protagonistas; se actualiza diariamente con contenidos originales. No obstante, sitios de los más variados temas han sido alcanzados por este error de indexación, abarcando incluso a autoridades del desarrollo web como www.seochat.com y www.webmasterworld.com.
Los números de Musica24 revelan a simple vista su dependencia en la forma en que aparece listado en Google, debido a que vio caer drásticamente sus visitas a partir del momento en que cayó al pozo de las páginas suplementarias. Una vez fuera, su tráfico volvió a la normalidad. Muchos empresarios de Internet manifestaron su preocupación en este marco, en el sentido de plantearse medidas ante la baja de visitas: 'tendré que despedir a varios empleados a menos que nuestra Web logre regresar a las posiciones que tenía en Google'. Una semana típica, de lunes a domingo, antes y después de estar en el "Club de las Páginas Suplementarias", como muchos lo han denominado.

Páginas vistas	Visitas únicas
14,353	3,215
14,100	3,096
13,810	3,046
15,755	3,250
17,895	3,524
14,942	3,176
13,946	2,757



Mientras Musica24.NET fue afectada, lo cual ocurrió del 6 de febrero al 17 de marzo, así era una semana típica -la diferencia en términos de visitantes diarios es clara-.

Páginas vistas	Visitas únicas
3,258	541
3,052	542
3,341	509
3,629	493
2,743	452
3,622	680
3,373	442

El motor de búsqueda número uno de Internet no sólo genera visitas a terceros, sino también ingresos, ya sea porque un cibernauta hace una compra en línea o porque se cruza con avisos publicitarios, ambos modelos propuestos por un sitio al que la persona llega tras hacer una consulta en Google.

Si su sitio no está en Google, ¿No existe?

Nadie puede depositar en Google el futuro de su emprendimiento virtual; no hay ninguna garantía de que lo conseguido no se perderá de un día a otro. Entre este año y el 2008 Google va a llevar a cabo cambios muy profundos, impulsados en gran medida por la competencia que librará Microsoft una vez que lance y consolide su nueva estrategia alrededor de Windows Vista.
Actualmente, los sitios Web reciben, en su mayoría, más del 85% del tráfico desde Google. Mientras tanto, Yahoo! y MSN representan cifras muy pequeñas. Sin embargo, no puede ignorarse el potencial de los motores de búsqueda que rivalizan con Google, menos aún cuando está próximo a desarrollarse el combate más desafiante del mercado de las búsquedas. Sin ir más lejos, ¿Alguien recuerda el alguna vez más importante buscador en el mundo, Altavista? Google ha construido un imperio que no será fácil de desarmar, pero un mercado más equilibrado, con más opciones líderes, siempre es bienvenido tanto por los desarrolladores como por los navegantes.

A almacenar...
...que se acaba el mundo.

Hoy el almacenamiento forma parte de la seguridad del negocio, al mismo nivel que los antivirus, antiespam, y otras herramientas antimalware, ya que todas constituyen la protección de la información. Y aunque suene a perogrullada, todo buen proyecto debe contemplar siempre una instancia de almacenamiento.



Ricardo D. Goldberger
Periodista Científico
Especialista en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos, conduce *"El Explorador Federal"* por AM Radio El Mundo y colabora en Gillespi Hotel, en FM Rock & Pop.

Hace algunos años, más exactamente en el 2002, se conoció un estudio que EMC, la empresa de soluciones de storage, le encargó a la Universidad de Berkeley acerca de la cantidad de información que el hombre había generado desde que comenzó a dejar señales en las paredes de las cavernas, hasta nuestros días.

La cantidad de información, medida en gigabytes, fue inmensa y no viene al caso. Lo que sí viene al caso es que la cantidad de información que se había generado desde el año 1995 hasta la fecha, había sido prácticamente la misma que se había creado desde la época de las cavernas hasta 1995. Peor aún, según la curva proyectada, para el año 2006, o sea éste, la cantidad se iba a duplicar. En otras palabras, el hombre habría generado en sus últimos diez años el doble de la información que generó desde la prehistoria hasta acá.

Es una pena que el estudio no se haya actualizado (sería bueno ver si EMC saca algunos mangos del bolsillo corporativo para hacerlo), pero aún cuando los datos no estén al día, lo cierto es que el fenómeno del almacenamiento se ha colocado en una ola de crecimiento asombrosa.

Mientras tanto, la avidez de las empresas por más y más información ha hecho que se desarrollara ingente cantidad de herramientas para adquirirla, procesarla, analizarla… y almacenarla.

La mayor parte de estas tareas/herramientas de software se escudan tras siglas tales como CRM, ERP, BI… y siguen las firmas. Cada vez son más los datos que se exigen de los clientes y cada vez más son las variables y parámetros que se incorporan al estudio de los procesos de negocio. A veces hasta exageradamente, pero se recolectan.

Todo eso exige no sólo espacio de almacenamiento, sino también herramientas para administrar ese almacenamiento. De nada vale que guarde un dato si después no tengo manera de acceder a él.

Para empeorar la situación, con almacenar la información una sola vez, no basta. Como la información es vital para el negocio -según algunos, es imposible hacer ningún negocio sin información- hay que tomar medidas de contingencia ante la posibilidad de que suceda algo que dañe esa información. Lo que va desde la rotura de un disco rígido hasta el robo a través de Internet.

Ahí es donde entra a tallar el backup, el famoso backup. Quizá la forma más sencilla y obvia de recuperar datos perdidos sea volver a traerlos desde una copia hecha antes de que esos datos se pierdan… lo cual implica que tenemos que pensar que los datos se pueden dañar **antes** de que les pase.

Pero además, y como si esto fuera poco, si perder los datos trastorna el negocio, perder **todos** los datos, lo trastorna **irremisiblemente**. Antes de que el desastre ocurra, uno tenía que haber tomado la precaución de establecer algún tipo de recuperación de desastres, algo que va más allá de un simple backup.

El estado actual de la economía globalizada, donde la cantidad de datos que se exigen no sólo es monstruosa sino que la mayor parte de las veces, tiene múltiples orígenes, explica suficientemente bien porqué en estos últimos años, la inversión en almacenamiento ha ido creciendo incesantemente. Como dato ilustrativo, valga comentar que en nuestro país, en los años 2002 y 2003, o sea, después de nuestra crisis económica de salida de la convertibilidad, la inversión en tecnología que menos cayó fue, precisamente, la inversión en almacenamiento.

A esta altura del partido, y con varias tecnologías que se han ido asentando con el tiempo (NAS, SAN, virtualización, etc.), el almacenamiento se ha ido convirtiendo en un elemento más de la ecuación que hay que hacer a la hora de presupuestar una solución. Cualquier proyecto que se precie debe tener un ítem que se refiera al almacenamiento, a la protección y a la recuperación de datos ante desastres. Y eso no hay que perderlo de vista.

demasiada información?

poweredbycisco.

Más clientes. Más información.
Y con ella más demanda para su DataCenter.
Como mantener esa información accesible y manejable en todo momento?
Y como hacerlo de manera óptima?
Conozca como la estrategia Cisco Service Oriented Network Architecture (SONA)
puede ayudarlo a evolucionar hacia una Red Inteligente de Información (IIN)
y así poder optimizar su infraestructura, aplicaciones y procesos de negocios que permitirán
al departamento de IT tener un mayor impacto en su empresa.

Lo invitamos a participar del evento exclusivo sobre soluciones para DataCenters que se llevará a cabo el día 18 de abril en el Hotel Sheraton.
Por favor confirme su asistencia al centro de atención al cliente:
0810-444-CISCO (24726)
o por mail a ciscoresponde@external.cisco.com



Evolución de los Sistemas de Storage



por **Robert J.T. Morris** y **Brian J. Truskowski**

Los Sistemas de storage (storage systems) se construyen basándose en las capacidades básicas de un dispositivo de almacenamiento (storage device), tal como un disco rígido (Hard Disk Drive, HDD), y agregando capas de hardware y software de modo de obtener alta disponibilidad, alta performance y fácil administración.
Sistemas de storage hoy soportan una variedad de servicios adicionales y alternativas de conectividad e interfaces.

En este artículo se mostrará como los sistemas de storage han evolucionado en las últimas cinco décadas, siempre buscando satisfacer las necesidades de los clientes. Primero se verá como fue el desarrollo de la unidad de control, las tecnologías RAID (Redundant Array of Independent Disks), servicios de copiado, y tecnologías de administración del storage. Luego, se describirá como el surgimiento de infraestructuras de redes locales (LANs) de bajo costo han permitido el desarrollo de las tecnologías "Network Attached Storage" (NAS) y "Storage Area Network" (SAN). Se explica como virtualización y File Systems (Sistemas de Archivos) SAN son necesarios para poder aprovechar al máximo los beneficios de éstas tecnologías.
Discutiremos como la tendencia actual hacia la administración de complejidad, facilidad de uso y reducción del TCO (Total Cost of Ownership) ha conducido al desarrollo de la virtualización del storage. También comentaremos brevemente sobre los desafíos y esfuerzos hacia el futuro.

El presente artículo ha sido realizado como un resumen del excelente artículo de R.J.T. Morris y B.J. Trwskowski y publicado en el IBM Systems Journal VOL: 42 Nº 2, 2003.

I) Los componentes

El primer dispositivo de almacenamiento de datos fue introducido por IBM en 1956. Desde entonces ha habido un progreso destacable en tecnologías de disco rígido (HDD).
Para entender la evolución de los "sistemas de storage" es importante conocer la evolución de los HDD. La densidad superficial de un HDD ha aumentado en siete órdenes de magnitud (10**7) y esto ha traído aparejado una reducción del espacio utilizado, también por el mismo factor. La figura 1 muestra la densidad superficial del HDD y el precio de los dispositivos de storage desde 1980. El precio de los HDD ha disminuido en cinco órdenes de magnitud (10**5) desde 1980, mientras que el costo de "sistemas de storage" han caído cerca de 2.5 órdenes de magnitud en el mismo período. La caída más rápida del precio de HDD implica que cada vez afecta menos en el costo total de un sistema de storage.
Aunque la ley de Moore dice que el número de transistores por unidad de área del silicio se duplica cada 1.5 años, la Figura 1 muestra que el número de bits almacenados por unidad de HDD se duplica cada año! Pero más importante que mejoras en densidad del dispositivo o costo, es el hecho de que nuevas aplicaciones han sido introducidas por éstos avances. En la línea de tiempo de la Figura 1, dos eventos sobresalen. En 1996, el almacenamiento digital se hizo más rentable para almacenar datos que el papel y en 1998 se alcanzó el punto en que las películas usadas en radiografías médicas podrían ser reemplazadas (por costo) por medios electrónicos. Otro hito, en este caso en el mundo de los consumidores, se alcanzó hace varios años cuando resultó más económico almacenar video usando sistemas de almacenamiento digital. Muy pronto aparecieron los "personal video recorders" basados en HDDs que además ofrecen un manejo mejorado.
Es instructivo también ver como soluciones de infraestructura son afectadas por el progreso relativo de las tecnologías.
La Figura 2 nos muestra los avances relativos en storage, procesadores y tecnologías de comunicación. En ésta se grafican mejoras en costo/performance de tecnologías de productos de usuarios finales mostrando como desde 1990, la tecnología de storage ha superado a las de comunicaciones y procesadores. Una historia paralela sucedió en el mundo empresarial: la cantidad de datos almacenados ha superado la habilidad de las comunicaciones y los sistemas de procesamiento para proveer fácil acceso a los datos. Por tanto, vemos un uso generalizado de múltiples copias de datos (replicación, caching de internet), como también implementación de sistemas de storage cerca del usuario, de modo de evitar demoras en la red.
El HDD representa cada vez más una parte más pequeña del sistema de storage (pudiéndose llegar al caso de ser 10% del costo). El valor pasó a las "advanced functions" y la integración de éstas con el sistema mismo. La Figura 3 es muy ilustrativa y nos muestra qué compraban U$D 3 millones en storage en 1984 y el año 2000.

II) De componentes a sistemas

Los primeros dispositivos de storage fueron directamente controlados por el CPU. La gran ventaja surje con la aparición de una unidad de control (controller) fue que los comandos I/O de la CPU (llamada host) eran traducidos independientemente a comandos específicos para el HDD. De este modo el HDD podía ser "controlado" independientemente y asincrónicamente de la CPU.
En los años 90 el storage dio un gran paso con la introducción de RAID que permitió la coordinación de múltiples HDDs de modo de dar mayores niveles de confiabilidad y performance que la de un dispositivo aislado. La aparición de dispositivos de almacenamiento más reducidos como discos de 5.25 pulgadas y 3.5 pulgadas, promovió el diseño de sistemas que usaban un mayor número de pequeños dispositivos. El concepto de paridad permitió el diseño de sistemas de almacenamiento que conti-

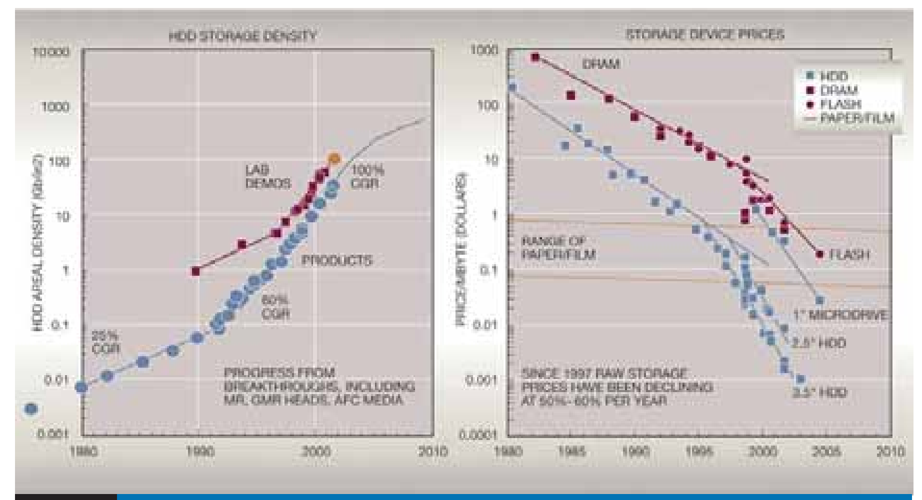


Fig 1. La densidad de almacenamiento en los discos rígidos, se está incrementando a un ritmo del 100% anual (actualmente supera los 100Gbit/inche2). El precio del almacenamiento está decreciendo rápidamente y ahora es significativamente más barato que el papel o el film.

nuaban operando aún ante fallas de discos.

El concepto de "Disaster Recovery" (Recuperación ante Desastres) apareció como un requerimiento en el mundo IT. Las soluciones podían pasar desde copias ocasionales a cintas magnéticas (transportadas manualmente) a versiones electrónicas del mismo principio, a soluciones de "mirroring" y verdaderos sistemas distribuidos. Varias tecnologías emergieron: 1) Una copia "point in time" (punto en el tiempo) que es hacer una copia virtual de los datos como aparecen en un dado punto de tiempo. Esta copia es mantenida actualizada siguiendo punteros a medida que se realizan cambios. Si fuese deseado, esta copia virtual puede hacerse una copia real a través de una copia física. 2) Mirroring (espejado) o copiado continuo que involucra dos copias espejadas de los datos. Una en un sitio primario (local) y otro secundario (de recupero). Se dice que este proceso es "sincrónico" cuando los datos son escritos en forma exitosa en el segundo sitio antes que la acción de "write" (escribir) dada por el primer sistema es confirmada como completa. Que el proceso sea sincrónico es lo deseado, pero es solo práctico sobre distancias cortas (aprox. 100 km). Por tanto otros esquemas "asincrónicos" son usados.

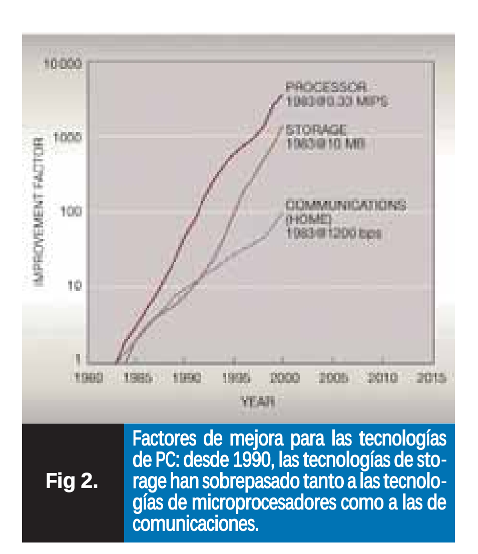


Fig 2. Factores de mejora para las tecnologías de PC: desde 1990, las tecnologías de storage han sobrepasado tanto a las tecnologías de microprocesadores como a las de comunicaciones.

Los requerimientos de disponibilidad de datos no estaban completamente satisfechos por sistemas de storage confiables, aún con infraestructuras redundantes de hardware y datos. Ya que los datos podrían ser borrados accidentalmente (por error humano o corrupción del software), copias adicionales eran necesarias con propósito de backup (resguardar). Los sistemas de "Backup" se desarrollaron de modo de permitir que los usuarios pudiesen hacer backups de archivos específicos o file systems completos. El método tradicional de backup fue usar cintas o, en el caso de computadoras personales, floppy disks o pequeños cartridges de cintas. Sin embargo, a medida que las redes se transformaban en ubicuas, backups basados en LAN fueron reemplazando metodologías basadas en cintas. Estas soluciones corrían automáticamente y en forma desatendidas. A veces, realizando backups de HDD a HDD.

Los sistemas de backup no son tan simples como parecen. Deben tratar datos con diferentes grados de importancia, en una variedad de clientes, servidores y dispositivos de storage y con un nivel de garantía que puede ser alto.

Por razones de performance y eficiencia, los sistemas de backup pueden proveer "backup incremental" (que involucra solo los archivos que se modificaron) y "file-differential backup" (que involucra sólo los bytes modificados en un archivo). Estas técnicas imponen un seguimiento muy alto en la integridad de los meta-datos asociados con los datos backupeados. Como las cintas aún proveen la forma más eficiente en costo/beneficio de guardar datos backupeados, hay un número grande de consideraciones relacionadas a la naturaleza de "append" (adjuntar) de los dispositivos de cinta que deben tenerse en cuenta.

Aunque el costo de almacenamiento en HDDs ha declinado enormemente, otros medios como cintas (tapes) o discos ópticos son usados e importantes. Por tanto, sistemas de storage basados en jerarquías que manejen éstos niveles de almacenamiento, son necesarios.

Además de aplicaciones en backups, los almacenamientos en cintas juegan un papel importante en operaciones de los data centres, con archivos que han sido migrados automáticamente por un sistema de administración de storage jerárquico y los llamados "master data sets" usados por ejemplo en procesamiento de tarjetas de crédito. Todas estas aplicaciones deben tener en cuenta el carácter secuencial de las cintas usadas en procesos "batch".

III) Network Storage

El surgimiento de tecnologías de red LAN de bajo costo constituyó el cambio más notorio en sistemas de storage de finales de los años 80 y principios de los 90. Las PCs fueron puestas en red y el modelo cliente servidor surgió. Aunque algún control sobre las aplicaciones migraron del data center a la PC, los datos más importantes tenían el status del recurso corporativo o institucional, más que un recurso personal y por lo tanto debía ser compartido y protegido. La PC era no administrable ni confiable y por lo tanto para tener datos compartidos, surgieron servidores de storage (de algún modo rudimentarios) basados en PCs y de bajo costo. Estos sistemas eran más de "misión crítica" que el cliente basado en PC y por lo tanto candidatos para tecnologías como File-Servers, RAID y sistemas de back-up en red (LAN). El sofware usado para networking era frecuentemente Novell Netware u otro software de algún vendor de PC. Al mismo tiempo, Unix sufrió un resurgimiento con las "Unix Workstation" (una alternativa al cliente PC) y server UNIX. La muy difundida disponibilidad de los protocolos para compartir archivos del NFS (Network File System) llevó a la aparición de file servers especializados.

El siguiente paso fue el surgimiento de sistemas NAS (Network Attached Storage), que brindaban un paquete que incluía la capacidad de file server en red contenido en una caja especializada, proveyendo protocolos de acceso standard como NFS, CIFS (Common Internet File System), HTTP (Hyper Text Tranfer Protocol) y FTP (File Transfer Protocol). Los sistemas NAS eran sencillos de implementar ya que se ofrecían como dispositivos empaquetados, completos con utilidades y funciones de administración.

Al mismo tiempo las organizaciones IT trataban de volver a tener el control sobre los "activos" dispersos, tan característico de la computación cliente/servidor. El data center volvió a tomar importancia en la mayoría de las empresas. Para este fin,

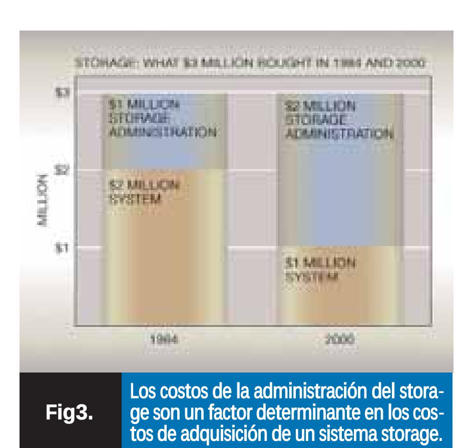


Fig3. Los costos de la administración del storage son un factor determinante en los costos de adquisición de un sistema storage.

FOOTBALL UNITES THE WORLD, AVAYA CONNECTS IT.

Lleve a su empresa a su máximo potencial de rendimiento.



Conozca todo lo que las Comunicaciones Inteligentes pueden hacer por Usted.

El próximo **23 de mayo**, tendrá la posibilidad de saber cómo es posible transformar su negocio, acelerar el crecimiento de su compañía, generar lealtad comercial y diferenciarse de sus competidores.

Somos proveedores oficiales de la red de comunicaciones más grande de la historia de los eventos deportivos: la **Copa del Mundo de la FIFA 2006™**.



RESERVE SU AGENDA. Regístrese pronto, los cupos son limitados.

0800 - 222 - AVAYA • mktgconosur@avaya.com

23 DE MAYO
SHERATON HOTEL

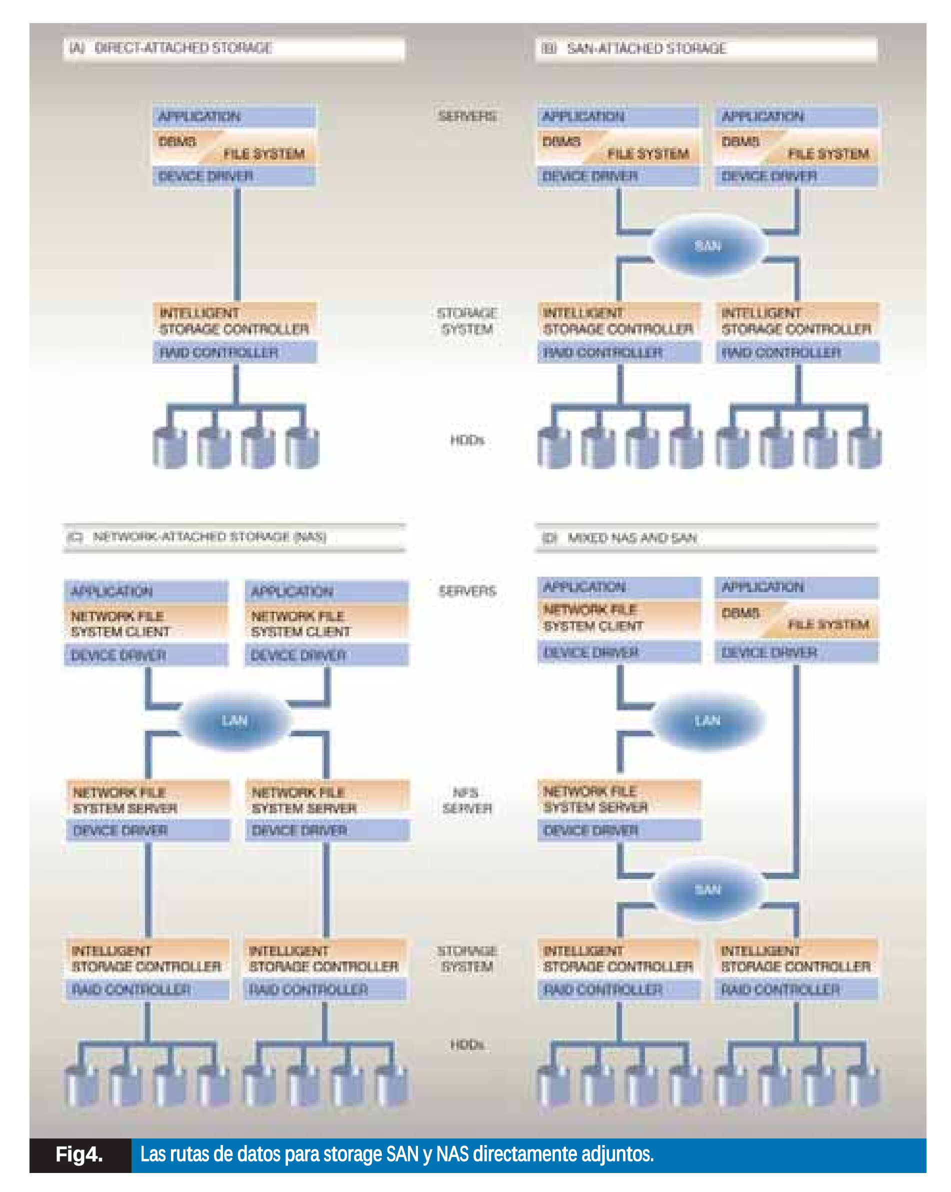


Fig4. Las rutas de datos para storage SAN y NAS directamente adjuntos.

servidores múltiples en un cuarto especializado buscaban la posibilidad de acceder a un storage back-end sin la necesidad de tener almacenamiento individual directamente "attacheado" y por lo tanto a un servidor individual. Ésto llevó al surgimiento de SAN (Storage Area Network).

Las SANs tenían la ventaja de que los sistemas de storage podían ser manejados separadamente de los servers. Esto permitía el "pooling" de storage (configurado estáticamente) resultando en eficiencias mejoradas y disminución de riesgos para el cliente (la inversión en storage no estaba condicionada a un hardware de server o un software particular). La tecnología SAN abrió nuevas oportunidades en conectividad simplificada, escalabilidad y manejo de costos y funcionalidades más dúctiles. Fiebre Channel se transformó en la tecnología de networking predominante. Para evitar confusiones el lector puede pensar a sistemas NAS como trabajando con archivos y protocolos de acceso a "block storage" (los bloques de datos pueden ser almacenados en el sistema de storage o en un HDD). Esta diferencia se ilustra en la figura 4 que muestra el "data-path" para DAS (Direct -attached storage) (A), SAN (B), NAS (C) y un entorno mixto de NAS y SAN (D).

La popularidad de redes Ethernet bajo TCP/IP ha llevado a un gran interés en su uso en la SAN. Tener las redes unificadas bajo TCP/IP y Ethernet ofrece beneficios de estandarización, mejores posibilidades de innovación y costos más bajos tanto en hardware y soporte de los dispositivos. Es así que aparece el Standard iSCSI (Internet Small Computer System Interface) que permite que el protocolo SCSI sea transportado sobre una red TCP/IP.

Aunque la disponibilidad del almacenamiento en red daba un acceso mejorado a los datos, aun dejó algunos temas importantes para resolver. Con SAN es posible una conectividad arbitraria entre el sistema cliente y el storage, creando problemas operacionales adicionales. Aunque en una SAN no hay una conexión directa (hard-wired) a su storage attacheado, está aun soft-wired, en el sentido de que la configuración es típicamente estática. Es imposible hacer cambios al "attached-storage" o sistema que la usa sin interrupción.

La adición de una capa de redireccionamiento entre el storage y el sistema que lo usa, puede ser provista por un switch de harware o un sistema intermediario de software, le permite al sistema cliente (típicamente un server) manejar cambios no disruptivos en la configuración del storage.

Adicionalmente, volúmenes virtuales pueden ser creados que abarquen múltiples dispositivos de storage. Ésto se conoce como "virtualizacion" y permite a todo un storage en una SAN ser considerado en un pool y luego disponible para acceso por los sistemas clientes. Esto también simplifica varios tareas en la administración del storage, como servicios de copiado, cambios de dispositivo on line y off line y otras. Pero el acceso no es suficiente, porque los sistemas cliente muchas veces tienen solo acceso a datos y no están equipados a compartirlos o el espacio libre que poseen. Por tanto, cada sistema tiene designada su propia cantidad de espacio libre, lo que representa un esquema de derroche de recursos. Este problema puede ser subsanado removiendo la tarea de administrar los meta-datos a cada uno de los sistemas clientes y creando una capacidad global que administre el mapeo, el compartir, y manejo del storage en todos los dispositivos attacheados. Además de simplificar la configuración y la administración del espacio libre, nuevas características pueden adicionarse como el compartir datos y la automatización de muchas funciones de la administración del storage. Este concepto se lo conoce como un "SAN file System".

Resumiendo: los sitemas de storage utilizan RAID para mejorar funciones básicas de los HDD (discos rígidos) y explotan tecnologías de red LAN en una SAN para ganar conectividad física con una variedad de dispositivos de storage. Pero la evolución actual va más allá. Virtualización nos provee un mapeo flexible lógico-a-físico en los dispositivos de storage y un file system común con administración de meta-datos separados y consolidados, lo que permite una administración dinámica basada en políticas y otras características adicionales en un entorno heterogéneo de sistemas. Las herramientas de administración de sistemas usan estas capacidades de modo de facilitar las tareas de administración de recursos de los administradores de sistemas. ■


Dr. Robert J.T. Morris
VP, Personal Systems & Storage
Director, Almaden Research Center
IBM Research


Brian J. Truskowski
Vice President and Chief Information Officer IBM Corporation

Virtualización del almacenamiento

Hitachi Data Systems, experimenta actualmente un fuerte crecimiento a nivel mundial, impulsado por las ventas de las soluciones basadas en la revolucionaria Plataforma Universal de Almacenamiento Hitachi TagmaStore, de su único controlador basado en aplicaciones de Virtualización - el software de gestión HiCommand - y por su nueva y amplia oferta de productos de gama media. En este artículo podremos entender la importancia que Hitachi Data Systems pone en el concepto de virtualización.

Definición

La virtualización es el proceso de lograr que uno o varios componentes físicos aparezcan como entidades lógicas simplificadas. La virtualización oculta la complejidad de la infraestructura subyacente para administradores, usuarios y aplicaciones. La virtualización del almacenamiento crea volúmenes lógicos de almacenamiento a partir de un grupo compartido de recursos de almacenamiento. Con la virtualización del almacenamiento de Hitachi, estos recursos de almacenamiento pueden incluir almacenamiento heterogéneo.

El punto de la virtualización del almacenamiento es simplificar las cosas. Resulta irónico que la virtualización se haya convertido en un tema de discusiones complejas y técnicas entre los proveedores de almacenamiento con diferentes modos de tratar la tarea. Es probable que el típico consumidor de almacenamiento, que busca la forma de simplificar el entorno de almacenamiento, decida rápidamente que la virtualización es demasiado compleja de implementar.

Esta discusión se ha centrado en dónde realizar la abstracción lógica o la virtualización del almacenamiento. Una respuesta es realizarla en el servidor host (software de volumen lógico). Este enfoque fue conocido en el entorno DAS, pero la evolución del almacenamiento en red lo hace problemático, ya que es probable que muchos servidores host tengan que acceder a un mismo grupo de almacenamiento. Otros proveedores recomiendan integrar la virtualización en dispositivos de virtualización dedicados o en los conmutadores de red. Cada uno de estos enfoques tiene sus ventajas y desventajas: la mayoría supone más complejidad a la infraestructura o restricción de las opciones de infraestructura para determinados proveedores.

Las preguntas críticas

En los últimos 5 años los clientes corporativos han visto crecer sus necesidades de espacio de unas pocas decenas de terabytes a cientos. Como ningún otro recurso de TI, los datos, son constantes en su crecimiento. En los próximos 5 años es razonable predecir que los clientes estarán almacenando petabytes, con un horizonte próximo de exabytes.

En este contexto, se presentan algunas preguntas críticas para los administradores de recursos de TI en las empresas que es clave tener en cuenta:

- ¿Cómo gestionar tal magnitud de información de almacenamiento y al mismo tiempo asegurar su integridad, accesibilidad y continuidad, cuando los desafíos de la tecnología y el negocio cambian



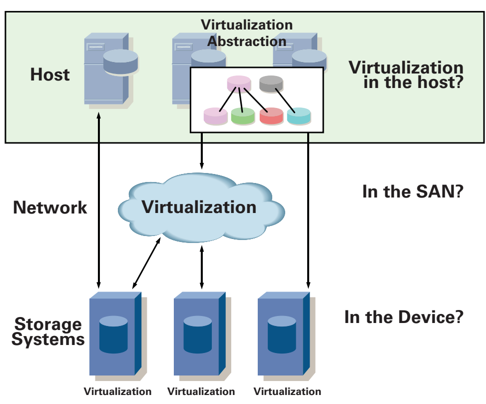
rápidamente?
- ¿Cómo realizar back up de cientos de terabytes cada día, conservando además el tiempo para procesar la información?
- ¿Cómo retornar a la operatoria normal luego de una interrupción del sistema que destruya un petabyte de datos?
- ¿Cómo manejar cientos de terabytes de datos de aplicativos, cumpliendo con diversos objetivos de forma simplificada y al mismo tiempo optimizar el valor de esas mismas aplicaciones de negocios?
- ¿Cómo cumplir con las regulaciones de la industria y del gobierno que requieren mantener almacenados los datos seguros por períodos que exceden la vida útil de los equipos de hardware de almacenamiento?
- ¿Cómo mantenerse actualizado con la tecnología que avanza cada 12 o 18 meses cuando las reglas de inversión y gestión de activos imponen cumplir con la capitalización de las inversiones de 3 a 5 años?
- ¿Cómo mover cientos de terabytes de una generación de productos a la siguiente sin impactar en las operaciones diarias que se realizan en línea?
La plataforma Universal de Storage de Hitachi está precisamente está diseñada para dar respuesta a estas preguntas a través de la implementación de virtualización de storage.



El enfoque de Hitachi: virtualización desde el controlador

Con la plataforma universal de almacenamiento, Hitachi integró la virtualización del almacenamiento en el controlador de almacenamiento. El controlador puede crear almacenamiento virtual no sólo para el almacenamiento interno, sino también para el almacenamiento de conexión externa, que puede incluir almacenamiento de terceros conectado al dispositivo. El sistema NSC55 extiende la virtualización desde el controlador del mercado para empresas hasta el mercado de almacenamiento convencional de capacidad media.
Este enfoque revolucionario sobre la virtualización del almacenamiento es único en el mercado. Gracias a que el controlador administra la virtualización, ni la aplicación ni el propio almacenamiento tiene que "preocuparse" de la tecnología de virtualización. **La virtualización del almacenamiento no significa más complejidad para la infraestructura de almacenamiento.**
El enfoque de Hitachi presenta varias ventajas sobre otras tecnologías de virtualización:
- No requiere conmutadores o dispositivos externos, ni software alojado en el servidor host.
- No depende de una red de almacenamiento; no es necesario comprar conmutadores nuevos ni cambiar la SAN para utilizar el sistema. Ni siquiera es necesario contar con una SAN; la virtualización desde el controlador también admite DAS en sistemas abiertos y entornos mainframe.
- Cómo funciona en el controlador de almacenamiento, la virtualización desde el controlador ya es compatible con el software de almacenamiento que usted puede estar usando, incluida toda la suite de soluciones de almacenamiento de Hitachi.
- Prolonga la vida útil de los sistemas de almacenamiento existentes y heredados, que pueden ser parte del grupo de almacenamiento virtual mediante la conexión a un sistema NSC55.
- Los administradores de almacenamiento pueden utilizar un único conjunto de herramientas administrativas para gestionar el almacenamiento heterogéneo; de este modo, se simplifica el almacenamiento considerablemente.

La importancia de la Virtualizacion de acuerdo con la visión de Hitachi Data Systems, es su impacto en el negocio de las compañías, pues al mejorar y automatizar tareas de gestión comunes en sistemas de almacenamiento heterogéneo, la Virtualización y el software asociado pueden reducir el costo total de propiedad para usuarios empresariales hasta en un 40%, de acuerdo con la consultora independiente ITCentrix. La reducción de costos se alcanza no sólo gracias a una mejor productividad en la administración, sino también reduciendo los costos de licencia de software tradicionalmente asociados al mantenimiento de



Dónde debería residir la Virtualización?

copias múltiples y gestión de productos, así como gracias a una eficaz gestión del ciclo de vida de los datos.
De acuerdo con los últimos informes de la firma IDC, las empresas necesitan nuevas tecnologías para optimizar la integración de sus recursos de IT, aprovechar al máximo su uso, facilitar la administración y asegurar su disponibilidad. Para ello, requieren soluciones que les permitan: Desplegar distintos niveles de almacenamiento optimizado de acuerdo a atributos específicos como performance, capacidad, disponibilidad y costo, replicar datos entre sus sistemas para que la gerencia de TI pueda moverlos en forma rápida e inteligente entre los diferentes tipos de almacenamiento, así como automatizar el aprovisionamiento, la expansión y la protección de los datos entre los sistemas de almacenamiento heterogéneos.

Claus Mikkelsen en Argentina

Claus Mikkelsen, actual Director Senior y Jefe Investigador de Aplicaciones de Almacenamiento de Hitachi Data Systems, y uno de los "padres" de la tecnología de virtualización estuvo en Argentina presentando ante un nutrido grupo de ejecutivos de sistemas y seguridad de empresas nacionales, que demostraron el creciente interés del mercado local por estas soluciones.
El reconocido investigador explicó que "Las soluciones de Virtualización brindan a las compañías la posibilidad de combinar y compartir sus recursos (de TI), además de hacer más eficiente su uso y suministro para satisfacer la demanda de los usuarios".
"Ésto es posible al combinar y reunir los servidores, el almacenamiento, la red y otros dispositivos que forman su estructura, y compartirlos a través de las aplicaciones y procesos de negocios, la Virtualización posibilita una respuesta rápida a los cambios que van desde las cargas de trabajo hasta las estrategias de la empresa, mercados o en la base del cliente," concluyó.
Si le interesa storage y en particular Disaster Recovery Planning no deje de conocer su blog:
http://blogs.hds.com/claus/



Storage basado en Grid

por **Abbot Schindler**

Mito o Realidad

Existen ideas erradas sobre Storage basado en Grid que están circulando por el mundo de los negocios. Muchos encargados de Storage todavía ven al Grid como una tecnología futura. Pero varios vendors están hoy, hablando del Storage en Grid y muchos de ellos están poniendo ya la etiqueta de Grid en productos específicos.
¿Cuál es la verdadera situación acerca de Storage basado en Grid? Descubra en este artículo los "Mitos y Realidades", en el cual presentamos los "facts"del Storage basado en Grid.

Visión del punto de vista del Bussines

MITO: el Storage basado en Grid continúa siendo una tecnología futura. No es nada que se necesite considerar por ahora.

REALIDAD: Usted puede comenzar a obtener las ventajas del Storage basado en Grid hoy.

Grid significa muchas cosas distintas a mucha gente diferente. Mientras que no hay una definición a nivel industrial de un Storage basado en Grid, muchas empresas están trabajando juntas para desarrollar una comprensión en común de esta tecnología. HP está desempeñando un papel clave en este proceso de desarrollo, junto con la Storage Networking Industry Association (SNIA), el Global Grid Forum (GGF) y otros.

HP ve al storage basado en Grid, como el modo más apropiado para llevar a cabo una infraestructura de storage, una que sea compuesta por componentes de hardware y software trabajando juntos para enfrentar las necesidades cambiantes del servicio de storage a través de organizaciones y de geografía.

Ciertas cualidades estarán presentes en cualquier solución de storage basado en Grid, incluyendo una arquitectura flexible y escalable, la arquitectura orientada a servicio (SOA), la habilidad de entregar conjuntos de capacidades de storage y administración de sistemas únicos. Estos elementos se encuentran ya integrados en varios de los productos de Storage de HP, por ejemplo:

- El HP StorageWorks Reference Information Storage System (RISS), el primero de la empresa en ofrecer Grid habilitado, es una arquitectura escalada que brinda alta performance, servicios de información rápidos y fáciles que se adaptan a las cambiantes necesidades de los negocios. RISS es una solución de "active-archiving" que ayuda a obtener más provecho de los datos, permitiendo acceder a éstos rápidamente mientras los protege de pérdidas.
- El HP StorageWorks Enterprise File Services Clustered Gateway provee una performance superior que escala el servicio de archivos y la carga de trabajo, mientras mejora las SANs existentes y nuevas. Usa componentes estandarizados industrialmente que son unificados y administrables como un solo sistema. Lo mismo se aplica al HP StorageWorks Scalable File Share (SFS), una poderosa solución de servidores de archivos que les da a los usuarios de clusters Linux, storage escalable y de alta performance que es fácil de usar y administrar. Los productos de storage basados en Grid como éstos, brindan medios para responder a la volátil capacidad IT, y requerimientos de performance, facilitando enfrentar los cambios que las empresas necesiten.

Las buenas noticias son que su compañía puede implementar storage basado en Grid de HP hoy mismo para poder disfrutar de los beneficios ahora -escalabilidad para performance y capacidad, como también administración simplificada de sistemas de storage Grid y algunos de los servicios especializados que ellos proveen- mientras puede continuar monitoreando la evolución de futuras tecnologías de storage Grid.

Vision del punto de vista IT

MITO: el Storage basado en Grid será una tecnología propietaria y competirá con su inversión en SANs.

REALIDAD: el Storage basado en Grid puede coexistir fácilmente con sus inversiones actuales del almacenaje en red, soportara los mismos protocolos y estándares que usted utiliza hoy.

Los productos de Storage basados en Grid de HP pueden conectarse fácilmente en la infraestructura del storage actual, por lo tanto no será necesario sustituir los sistemas existentes del storage tales como redes del almacén (SANs) y network-attached storage (NAS). Las semejanzas entre Grid y los ambientes de Storage que lo precedieron, permiten conexiones lógicas.

La diferencia principal es que el Storage basado en Grid puede hacer más en un ambiente de administración simplificado que el SAN. Storage basado en Grid combina el enfoque "scale-up" y "scale-out" para ofrecer niveles de performance de storage más altos. Y al ser una arquitectura orientada servicio, el storage basado en grid le permite en última instancia manejar y ajustar más fácilmente el storage para cumplir con los variables acuerdos de niveles de servicios (SLAs).

Mientras tanto, HP, junto con SNIA, GGF y otras entidades de los estándares de la industria, están trabajando para integrar el interfaz entre Storage y la computación en Grid para ayudar a asegurar la compatibilidad a lo largo de toda la cadena de recursos IT.

El storage basado en Grid, el SAN y la NAS son diferentes maneras de solucionar el mismo problema: ¿Cómo acceder a sus datos cuando los necesita? Su mejor opción es hoy comprar la solución más apropiada de Storage disponible cuando usted la necesita. Al mismo tiempo, observe cómo las definiciones de la industria y el rumbo que toman los productos alrededor de storage en grid, evolucionan. Estas direcciones ampliarán sus opciones en el futuro, así como le brindarán perspectivas útiles para las compras en curso de Storage y de la Administración.

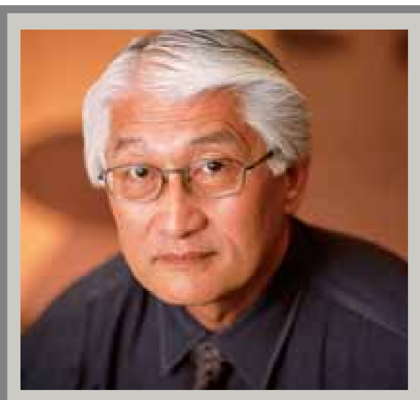
En cualquier caso, puede estar seguro que la coexistencia entre el Storage basado en Grid y otros tipos de Storage en red salvaguardarán sus inversiones actuales de Storage mientras accede al poder que le otorga Grid. ■



Abbot Schindler:

Es esperto en tecnología senior en Hewlett-Packard. Abbott ha estado involucrado con tecnologías avanzadas de storage por más de dos décadas. En su actual cargo, explora nuevas y emergentes tecnologías y cómo aplicarlas para obtener productos líderes en el mercado de storage en red, soluciones completas y estrategias. Está vinculado muy estrechamente con la estrategia de StorageWorks Grid de HP y otros esfuerzos de vanguardia de la empresa.
Abbott ha sido por más de una década un orador ampliamente reconocido. Ha dado conferencias en numerosos eventos alrededor del mundo, como también en eventos de Storage Networking World en Japón y Europa. Es también un frecuente orador en otras industrias y eventos de HP.

Virtualización de Servidores, de Storage y la computación como un "commodity"



Hubert Yoshida, es Vice Presidente y Chief Technology Officer y responsible de definir la dirección técnica de Hitachi Data Systems
http://blogs.hds.com/hu/virtualization/index.html

En varios artículos de NEX hemos tratado el tema de "virtualización de servidores" y en la idea de pensar a la computación como un commodity (Grid Computing). En un artículo en su blog, Hu Yoshida (Vice President y Chief Technology Officer de Hitachi Data Systems), discute estas ideas en vista del reciente anuncio de EMC de dar gratis su Virtual Server. Si desea ver como se juntan estos conceptos con la "virtualización del storage" lea lo que sigue.

Dice Hu Yoshida en su blog (Febrero 11, 2006):

"CNET publicó una nota el 2 de Febrero, en la que dice que EMC anunciaría esa semana que "regalarían" su Servidor GSX, que corre como en un host corriendo Windows o Linux y permite a sistemas operativos "guest" correr encima en máquinas virtuales. Esta jugada podría beneficiar a VMWare, al afianzar su liderazgo en virtualización de servidores por sobre tecnologías de desarrollo similares como la open source XEN, y Microsoft Longhorn Server. También establece una dependencia para incentivar migraciones hacia el servidor ESX enterprise, el cual es más caro, tiene más características y no requiere un host ya que corre debajo de la capa del sistema operativo (concepto de hypervisor).

Uno de los primeros en comentar sobre esto fue Nicholas Carr, conocido por "Does IT Matter" (http://www.nicholasgcarr.com/doesitmatter.html). Él cree que al hacer la virtualización gratuita, EMC hace de la computadora un commodity. "Crear servidores virtuales puede a fin de cuentas ser más valioso que armar el hardware en los que ellos corren". Él habla sobre las ventajas de la virtualización, commoditizar la computadora, y la llegada de una computación utilitaria más eficiente, y flexible.

Mientras estoy de acuerdo con que la virtualización de plataformas de servidores, creará una plataforma de computación más flexible y eficiente, no coincido en que la hará un commodity.

La virtualización sólo enmascara la complejidad, no la elimina. Consolidar una cantidad determinada de plataformas de servidores en una sola plataforma de cómputo (un único hardware), requiere una plataforma robusta de cómputo, que debe poder escalar, y prestar calidad de servicio por cada plataforma agregada.

Mientras la virtualización de un servidor tiene la intención de hacer ver a una computadora como si fueran muchas, y la virtualización de storage debe hacer ver a varios sistemas de storage como uno solo ambos, comparten el mismo desafío enmascarando complejidad. La virtualización solo enmascara la complejidad de la capa subyacente, pero no elimina la complejidad. La complejidad permanece y debe ser resuelta en la plataforma de hardware base. La virtualización de storage requiere de un motor de virtualiación, que escala a petabytes de storage y decenas de miles de plataformas de host, mientras le garantiza a cada usuario su propio espacio de storage seguro y calidad de servicio. Una plataforma de storage que pueda proveer ésto, no es un sistema commodity.

Poner un software de virtualización en una PC no brindará una solución de virtualización robusta y escalable. Las plataformas de computadoras y las plataformas de storage que no provean la infraestructura de hardware mejorada para virtualización, serán "commoditizadas", pero aquellas que sean mejoradas para virtualización prosperarán. El hardware sí importa.

Consolidación de servidores

En NEX #22 hablamos de Virtualización de servidores (VMware, Microsoft Virtual PC-Server…). Muchos nos preguntaron en qué contexto puede ésto ser útil/práctico. Las aplicaciones son variadas: entornos de simulación, educativos o aspectos de seguridad. Pero, quizás la "consolidación de servidores" en data centers sea la aplicación de más interés hoy. Los managers se enfrentan a la problemática de realizar planes de modo de consolidar el creciente número de servidores en sus data centers y saben que la virtualización es la mejor solución para ésto.

¿Cómo es de compleja, por ejemplo, una migración de diferentes servidores corriendo Windows Server 2003 o Linux en una sola máquina física?

Existen varias empresas (y sus softwares asociados) dedicadas a dramáticamente acelerar proyectos de consolidación de servidores reduciendo los tiempos de migración de meses a días. Lo hacen automatizando la medición, análisis y movimiento de cientos de servidores a entornos virtuales. Dan gran flexibilidad y gran ROI.

Si desea investigar más vea: (P=physical, V=virtualization): - www.leostream.com (producto: Leostream P>VDirect)
- www.vmware.com (producto: VMware P2V Assistant)
- www.platespin.com (productos: Power P2V 4.1 y Power Recon 1.0)

Xen hypervisor. Lo último open source en virtualización

En NEX #17 dedicada a "GNU/Linux y Open Source", en el artículo de la página 70 "The best of Open Source" hablamos muy someramente de Xen.

Xen es un monitor de máquinas virtuales open source (hypervisor). Fue desarrollado por la universidad de Cambridge, UK. Está diseñada para permitir correr 100 instancias de Sistemas Operativos en una sola computadora "estandard". Xen provee aislamiento seguro, control de los recursos, garantías de calidad de servicio (quality of service, QoS) y "live migration" (migración en vivo) de máquinas virtuales. Los sistemas operativos deben ser explícitamente modificados ("ported") para correr sobre Xen (aunque se mantiene compatibilidad para las aplicaciones de los usuarios). Ésto le permite a Xen lograr virtualizaciones con un alto grado de performance.

Las máquinas virtuales son usadas con frecuencia por IBM y otros vendors sobre sus mainframes y servidores para utilizar sus recursos al máximo y asegurar los programas poniéndolos en sistemas operativos virtuales separados, como en una cárcel chroot pero aún más. Puede ser usado no solo por razones de seguridad o performance, sino también para correr en la misma computadora Sistemas Operativos diferentes e incompatibles. El soporte de Xen para realizar "live migrations" de máquinas virtuales permite balance de carga y poder evitar downtime. Hasta ahora Xen no permitía correr Windows. Eso cambió.Quien desee ver últimas novedades sobre Xen y Windows lea: http://news.com.com/Xen+passes+Windows+milestone/2100-7344_3-5842265.html

Hay un artículo muy interesante en Linux Journal de Septiembre 2005: "Introduction to the Xen Virtual Machine", By Rami Rosen http://www.linuxjournal.com/article/8540#comment

Lea el artículo de Luis Otegui en NEX IT Specialist #21 "Linux y Seguridad, ¿El reposo del guerrero? Allí podrá entender como la idea de la virtualización influencia la seguridad de los SOs.

Viridian: un hypervisor de Microsoft

Microsoft está trabajando fuerte por tener una parte de la acción. En Diciembre, rebajó los precios del Virtual Server 2005 R2 de $999 a $199 (para la versión Enterprise Edition) y de $499 a $99 (para la Standard Edition). La Standard Edition corre en servidores con hasta cuatro procesadores, mientras que el Enterprise es para sistemas más grandes.

Mucha de la atención de Microsoft está dirigida al futuro con un sucesor, el Microsoft Hypervisor, (nombre código "Viridian"). Virtual Server necesita de Windows como soporte, pero los hypervisores son software de bajo nivel. Tanto el ESX Server como el Xen emplean el enfoque del hypervisor.

Un gran cambio que introduce Viridian será el soporte para máquinas virtuales de 64-bits. Ello pondrá a la par a Microsoft con Xen y VMware, lo cuales soportan máquinas virtuales 64-bit en la actualidad.

Es improbable que Viridian haga su debut hasta el 2008 como mínimo, sin embargo, está diseñado para funcionar con el esperado Longhorn Server, una versión orientada a servidores del Windows Vista cuyo lanzamiento está previsto para el 2007, aunque es más probable que sea incluido en un service pack entre 18 y 24 meses luego de su lanzamiento.

por **Tom Nosella**

Optimizando su SAN

para la continuidad de los negocios

Como cada vez es mayor el volumen de datos de storage que atraviesa la WAN, la demora ocasionada por la distancia, y las nuevas amenazas a la seguridad, están dando de que preocuparse. Las empresas deberían soportar las técnicas de aceleración de SAN, seguridad multifacética, y capacidades e interfaces de administración de estandarizadas industrialmente, para asegurar que su SAN se desempeñe bien y permanezca segura, con costos reducidos, y administrable.

La forma en que las empresas están implementando redes de storage está dando un giro. La razón es que esas redes han pasado a jugar un papel significativo ayudando a las organizaciones a asegurar la continuidad de los negocios durante fallos en los sistemas y caídas de sus sitios. Los backups de los datos eran, en un entonces, confinados a unos pocos servidores, cintas de datos, y switches (fácilmente controlados y asegurados en un solo data center). La seguidilla de recientes desastres naturales y otras emergencias ha causado que la mayoría de las empresas reconsideren este diseño.

Para protegerse mejor, más organizaciones están haciendo backup de sus datos en dos o más lugares y usando el protocolo TCP/IP para un acceso rápido y versátil desde sitios distribuidos. El uso, actualmente común de tecnologías de almacenamiento basadas en IP como Internet Small Computer System Interface (iSCSI) y Fibre Channel sobre IP (FCIP) permite que los usuarios sean automáticamente redireccionados a los recursos de back up en lugares geográficamente diversificados, en el caso de que los datos estuvieran inaccesibles en el sitio primario. Esta estrategia es una bendición para la disponibilidad de los datos; sin embargo, trae consigo algunas nuevas consideraciones para la red de backups.

Entre estas cuestiones se encuentran asegurar la performance del almacenamiento de datos a lo largo de enlaces distantes como también la seguridad de esos datos en tránsito y la escalabilidad de la huella del Storage-Area Network (SAN). En resumen, los managers de IT están comenzando a lidiar con muchas de las mismas cuestiones en sus redes de storage, que antes encontraban en sus redes de datos. Al igual que con las redes de datos, volúmenes cada vez mayores de datos de storage recorren la WAN, lo cual agrega un retraso causado por la distancia y nuevas vulnerabilidades de seguridad a la ecuación del diseño.

Los profesionales IT deberían considerar las siguientes cuestiones al montar SANs que podrían estar a miles de kilómetros de los sitios que intentan acceder a éstas:

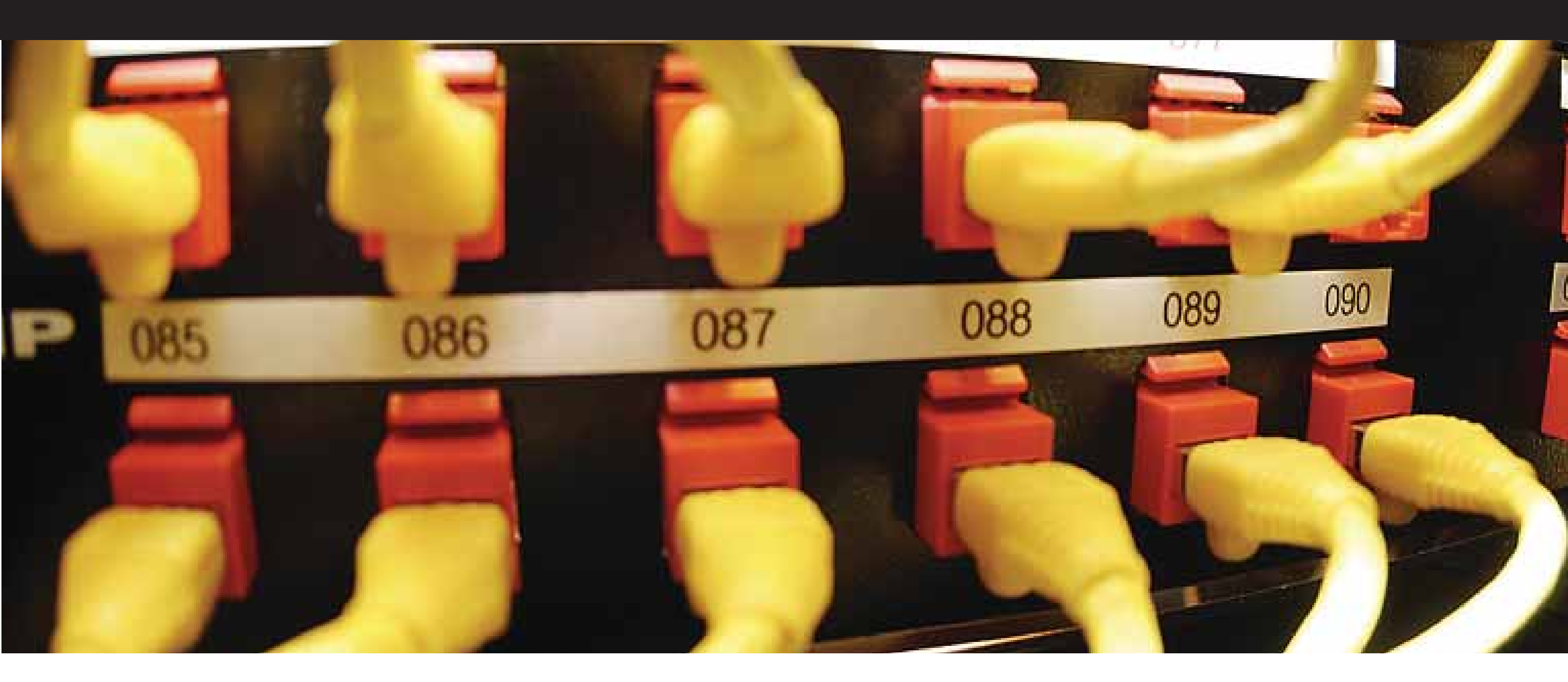
- ¿Hay manera de compensar el retraso inducido por la distancia, para acelerar la performance del SAN?
- ¿Cómo se puede asegurar los datos de storage que salen del data center y transitan redes de datos comunes, contra ataques, alteración, robos, o que sean interceptadas (eavesdropping)?
- ¿Cómo puede ser asegurada la autenticación fuerte y autorización de usuarios, dispositivos, y personal de administración IT?
- ¿Hay alguna manera de particionar el acceso a recursos SAN, de la misma manera que las Virtual LANs (VLANs) de Ethernet, particionan el acceso a servidores en vivo (live servers), usando grupos de usuarios lógicos para obtener escalabilidad, aislamiento de fallas, y seguridad?
- ¿Cómo manejan las organizaciones un ambiente SAN heterogéneo?

Una combinación de estándares industriales e interfaces, junto con características en los equipos de los vendors, ayuda a que los administradores IT aseguren la aceleración de la performance, la seguridad y la administración en la SAN para mejorar la continuidad de los negocios.

Acelerando la SAN

La aceleración en la SAN es conceptualmente similar a la aceleración de performance de aplicaciones en redes de datos. Sólo que en vez de realizar Proxy server, los protocolos de aplicación para reconocimiento local, son los mismos protocolos de control de SAN quienes son reconocidos localmente para reducir el número de viajes de ida y vuelta, y el tiempo asociado que lleva mover los bloques de datos del punta A al punto B. Por ejemplo, el protocolo SCSI requiere dos viajes de ida y vuelta de reconocimiento para cada operación de escritura. Cuando los dispositivos locales piden datos a una SAN lejana, aquellos dispositivos pueden ser reconocidos localmente para reducir la latencia inducida por la WAN.

Hay dos tipos de aceleración, o acknowledgement locales, predominantemente en uso: aceleración de escritura y aceleración de cinta. Su uso depende de qué tipo de medio de soporte vaya a ser accedido. Ambos son soportados por la familia de switches multiprotocolo para storage Cisco MDS 9000. Estos dispositivos soportan simultáneamente Fibre Channel, FCIP, iSCSI, y conexiones al mainframe vía Fibre Connection (FICON). Intercambian datos de Fibre Channel entre puertos semejantes y también encapsulan datos de Fibre Channel en IP y lo envían a una interfase Ethernet para tránsito IP. Ambos tipos de aceleración incrementan la performance.



Aceleración de Escritura: Esta mejora de reconocimiento usada para transmisiones de disco-a-disco y host-a-disco, reduce los viajes de ida y vuelta de los datos SCSI de dos a uno, por lo tanto duplicando la performance. En este caso, un reconocimiento del recibo de datos intactos es enviado luego del segundo viaje de ida y vuelta del proceso de handshaking.

Aceleración de Cinta: Esta mejora de reconocimiento parte de la aceleración de escritura, descripta arriba, para acelerar los datos de storage en movimiento desde un servidor de medios a una unidad de cinta. La performance es mejorada primero por reconocimientos locales que reducen el viaje de ida y vuelta de los datos por la WAN a la mitad. Sin embargo, un mecanismo configurable de marcado de archivos en los sistemas de cintas, le permite al Administrador IT establecer que el mecanismo de reconocimiento de larga distancia tenga lugar luego de un determinado número de bloques de datos, en lugar de luego de cada uno de los ellos, para reducir el número de reconocimientos aún más. Los datos son almacenados en un buffer entre cada reconocimiento. Como la velocidad del medio de almacenamiento en cinta es notoriamente lento, al reducir el reconocimiento requerido a cada X número de datos, se obtiene significativos beneficios en la performance. Por ejemplo, en algunos test hechos por consumidores de Cisco, un reconocimiento de 100 milisegundos tiene un impacto de tan solo 15% en la performance.

Compresión

Al igual que en las redes de datos, la compresión también puede ser usada para incrementar el ancho de banda efectivo de la WAN, evitar congestionamientos, y mejorar la performance. Los switches para storage de Cisco soportan diferentes algoritmos de compresión de datos, elegibles dependiendo de la configuración, que permiten cocientes de compresión (compression ratios) de hasta 30:1, dependiendo de la compresibilidad del paquete de datos. Los cocientes de compresión para el tráfico común de bases de datos son de entre 2:1 y 3:1.

Asegurando Datos de Storage

Las preocupaciones típicas de la seguridad de las redes, están comenzando a aplicarse a las SANs. Las SANs, generalmente han sido pequeñas y localizadas dentro de un solo data center. Ahora, sin embargo, redes que recorren mayores distancias y que usan varias estructuras de proveedores de servicio, deberán poder mover datos críticos que posiblemente nunca antes hayan salido de un data center, salvo en un soporte físico a bordo de un camión.
El resultado de este cambio en el tratamiento de datos almacenados es la necesidad de aplicar al ambiente Fibre Channel, las características de seguridad preexistentes en los elementos de redes IP. Ésto involucra la protección de datos en tránsito, asegurarlos contra accesos de usuarios y dispositivos no autorizados y protegiéndolos contra desconfiguraciones de administración maliciosas. En una red de switches de storage tales como Cisco MDS 9000, también llamados un "tejido de storage" ("storage fabric"), esto involucra encriptación, autenticación, y asegurar la infraestructura de administración de la SAN.

Encriptación

La encriptación es importante para prevenir que los intrusos vean o modifiquen información confidencial. Los switches para storage de Cisco usan el protocolo IPSec para ayudar a asegurar la confidencialidad e integridad de los datos en tránsito.
Los switches Cisco MDS 9000 multiprotocolo SAN, por ejemplo, incluyen encriptación/desencriptación de IPSec integrada en el hardware, soportando los algoritmos Advanced Encryption Standard (AES), Data Encryption Standard (DES), y Triple Data Encryption Standard (3DES) para tráfico de storage iSCSI y FCIP.

Autenticación y Autorización

Estas funciones son ahora necesarias para evitar la corrupción accidental y ataques maliciosos en datos SAN. Permiten conectarse a los datos almacenados sólo a usuarios y dispositivos certificados. La autenticación de storage Switch-to-Switch y la autenticación de otros switches conectándose a un tejido de storage de Cisco usan el criptográficamente seguro intercambio de llaves y compo-

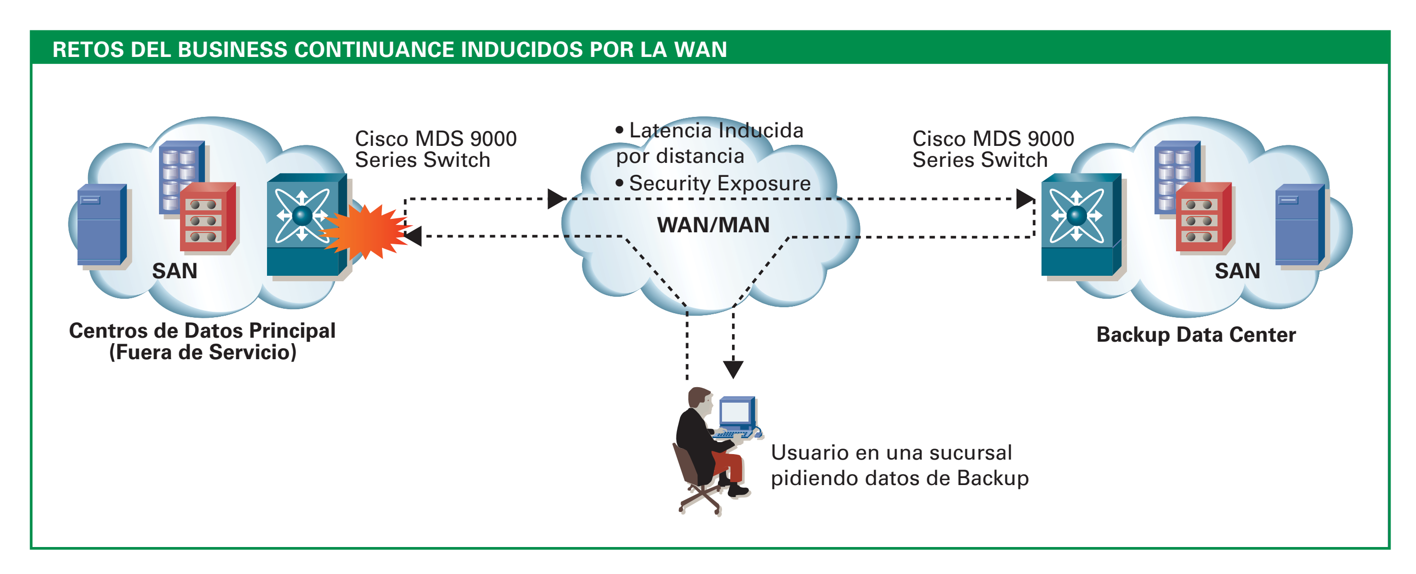
Léxico de Seguridad en Storage y Administración:

FC-FS-2 Fibre Channel-Framing y Signaling-2:
Especificación definida por el Technical Committee T11 del Internacional Committee para Information Technology Standard (INCITS) para transmitir comandos SCSI, datos, e información de estatus entre un iniciador SCSI y un objetivo SCSI.

FC-GS-3 Fibre Channel-Generic Services-3:
Es un estándar de administración definido por el Technical Committee T11, para transferir información de status y configuración, incluyendo información VSAN, entre dispositivos de Fibre Channel.

FC-SP Fibre Channel-Security Protocols:
Estándar en estado de borrador, creado por el Technical Committee T11 del INCITS, para asegurar datos de storage en tránsito por Fibre Channel usando encriptación de datos, intercambio de llaves criptográficamente segura, y autenticación de dispositivos. FC-SP es soportado por varios fabricantes de switches SAN y por todos los principales vendors de adaptadores de bus de host. Se espera su aprobación en Marzo de 2006.

SMI-S Storage Management Initiative Specification:
Es un estándar desarrollado por el Storage Network Industry Association (SNIA) que tiene la intención de facilitar la administración de dispositivos de storage de múltiples vendors en SANs, permitiéndole a una única aplicación de administración manejar múltiples tareas que de otra manera requerirían varias aplicaciones.



Las distancias considerables entre las SAN de los data centres, y entre las oficinas y los SANs, lleva a la necesidad del uso de la aceleración de performance de SAN, usando reconocimientos de protocolo de SAN locales. Los mecanismos de seguridad tradicionales deberían también ser agregados a los datos SAN transportados a través de la WAN.

nentes de autenticación de dispositivos de los protocolos de seguridad de Fibre Channel (Fibre Channel-Security Protocols [FC-SP]), un estándar del Internacional Committee para Information Technology Standard (INCITS) del Institute of American Nacional Standards, desarrollado por el comité técnico de T1. Las organizaciones pueden autenticar usuarios y dispositivos localmente en el switch de storage, reduciendo la latencia, o remotamente a través servidores de autenticación, autorización, y contabilidad (conocidos como servidores AAA).

Infraestructura de administración Segura

Las funciones de administración del data center concernientes a redes y dispositivos de almacenamiento, también deberá estar asegurada para frenar accesos no autorizados. Los usuarios maliciosos con acceso a la consola de un dispositivo de storage conectado a la red, puede fácilmente modificar configuraciones. Al igual que otros elementos Cisco para redes, el switch Cisco MDS 9000 brinda funciones administrativas seguras, incluyendo Secure Sockets Layer (SSL) y Protocolo Secure Shell Versión 2 (SSH), los cuales aseguran acceso seguro usando autenticación y encriptación. SSHv2 puede ser usado en conjunto con protocolos back-end de autenticación de usuarios, como TACACS+ y RADIUS que pueden estar ya implementados en la Organización. En este caso, el switch de storage actúa como cliente del servidor back-end AAA que corre estos protocolos.

Finalmente, el soporte de Simple Network Management Protocol version 3 (SNMPv3), permite autenticar y autorizar servicios para acceder a bases de información SNMP (SNMP management information bases [MIBs])

VSANs para Escalar y Aislamiento de Fallas

Una arquitectura virtual SAN (VSAN) bien planeada, reduce el total de SANs (o tejidos, fabrics) implementadas, mientras que permite separar sus backups, recuperación y dominios de mirroring de datos de SANs de aplicaciones específicas.

El año pasado, la tecnología de Cisco fue elegida por el Technical Committee T11 del INCITS como estándar para VSANs. Las VSANs permiten a los network administrators segmentar un único tejido físico SAN en varios lógicos, completamente independientes. Al igual que con las VLANs en una red de datos del tipo Ethernet, este enfoque permite la creación de dominios SAN separados sin tener que montar varias costosas infraestructuras físicas por separado.

Los dispositivos Cisco MDS 9000 pueden crear hasta 256 topologías VSAN aisladas (el hardware soporta una expansión de hasta 4096 dentro de la misma infraestructura física); ésto permite a los administradores usar delineamientos simples de zonas para restringir el acceso y flujo de tráfico entre dispositivos asegurando el acceso en los bordes. Los negocios pueden segregar incluso un solo switch de storage en múltiples ambientes virtuales, o dominios. Éstos pueden separar completamente las VSANs para ayudar a asegurar que la inestabilidad del tejido o la falla de un dispositivo sean aisladas dentro de una sola VSAN y no cause una interrupción extendida del tejido.

Administrando la diversidad

A medida que las redes de storage continúan creciendo, las organizaciones están implementando soluciones de storage usando equipos de varios vendors, los cuales vienen con sus propios programas de administración de SAN. Los administradores requieren una manera efectiva de manejar efectivamente el ambiente heterogéneo de storage de forma que aseguren una máxima performance y efectividad de costos.

El Cisco Fabric Manager para SANs les permite a los administradores ver y administrar los tejidos heterogéneos como una colección de dispositivos, recreando la totalidad de la topología y representándola como un mapa personalizable. Cualquier dispositivo en el tejido que soporte el estándar INCITS T11 Fibre Channel Generis Services-3 (FC-GS-3) para administración in-band puede ser descubierto y mapeado como parte de la topología. Una ventana de topología muestra los dispositivos descubiertos para personalizarlos y navegarlos, mientras que una ventana de inventario muestra una estructura de árbol de tanto elementos físicos como virtuales. Otra ventana muestra las herramientas que los administradores pueden usar para configurar, monitorear, y asistir a los dispositivos.

Cisco Fabric Manager también soporta interfaces abiertas con acceso a performance en crudo e información de configuración dentro de los switches, que puede ser usada por aplicaciones de administración de terceros. El soporte para Storage Management Initiative Specification (SMI-S) de la Storage Networking Industry Association, por ejemplo, permite la administración de elementos a lo largo de los productos de administración de SANs de múltiples vendors.

Las organizaciones que crean sus SANs buscando continuidad en sus negocios, se están encontrando frente a frente con muchas de los problemas centrales de las WAN como cuestiones concernientes a la performance, administración, y nuevos riesgos de seguridad, con los que se habían enfrentado previamente en sus redes de datos. ■

Acerca del Autor:



***TOM NOSELLA**, CCIE No. 1395. Director de Ingeniería en el grupo de Data Center, Switching, y Security Technology de Cisco.*

Redes SAN:

Rapidez, Seguridad y Flexibilidad para los datos de su empresa.

Alejandro Regueira
IT Regional Manager
XNET SOLUTIONS
una empresa del
Grupo LOGICALIS

Las operaciones de toda empresa moderna deben tener, como componente primordial, la administración de información. Las redes de almacenamiento modulares hacen que esa gestión sea más flexible y competitiva.

Nuevas soluciones de almacenamiento a medida

El activo estratégico de los negocios actuales es la información; de esta forma, el rendimiento de una solución de almacenamiento puede mejorar u obstaculizar el quehacer cotidiano en su compañía. La interacción entre aplicaciones y datos necesita de herramientas que permitan gestionarla eficazmente.
Independientemente del tamaño de una organización, todas se enfrentan con desafíos de almacenamiento similares: crecimiento exponencial de datos, mayores exigencias en cuanto a la disponibilidad y el desempeño de las aplicaciones, continuidad de los negocios, ventanas de respaldo más acotadas e infraestructuras de almacenamiento complejas y difíciles de manejar.
Las empresas medianas deben hacer frente a estos desafíos sin los recursos con los que cuentan las empresas de gran envergadura, porque tienen limitaciones presupuestarias, de personal y de espacio en el centro de datos, entre otros puntos relevantes.
Para resolver eficientemente esta problemática, se desarrollaron soluciones que permiten alinear los requisitos particulares de cada aplicación, a los atributos de almacenamiento. Estas soluciones se construyen sobre un nuevo conjunto de líneas de productos modulares que brindan confiabilidad, disponibilidad y desempeño superiores a los productos tradicionales o monolíticos, así como funciones de administración de almacenamiento de avanzada que por lo general no están disponibles en las soluciones monolíticas.

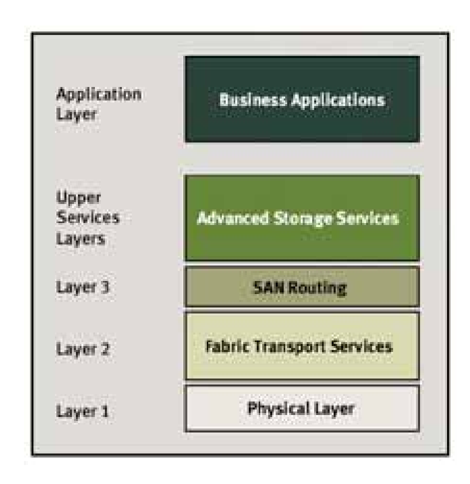
> "La infraestructura de almacenamiento debe estar alineada con las necesidades del negocio y las aplicaciones que utiliza cada empresa.

Redes de almacenamiento SAN

Las redes de almacenamiento SAN (Storage Area Network) permiten acceder y compartir grandes cantidades de datos en forma más rápida, simple y segura. Actualmente, representan la convergencia entre reservas de información y tecnologías de networking. Las SAN son redes de alta performance que tienen como objetivo principal el transporte de información entre sistemas computacionales y dispositivos de almacenamiento, y entre éstos últimos entre sí. Están compuestas por una infraestructura de comunicación, que provee las conexiones físicas y capa de transporte, y una capa de administración, que organiza las conexiones entre las aplicaciones y los dispositivos de almacenamiento.
Entre las ventajas que presentan, encontramos que: permiten la centralización de datos, acelerar los tiempos de respuesta para todo tipo de proceso de información y una alta disponibilidad de la información administrada.

Diseños monolítico y modular

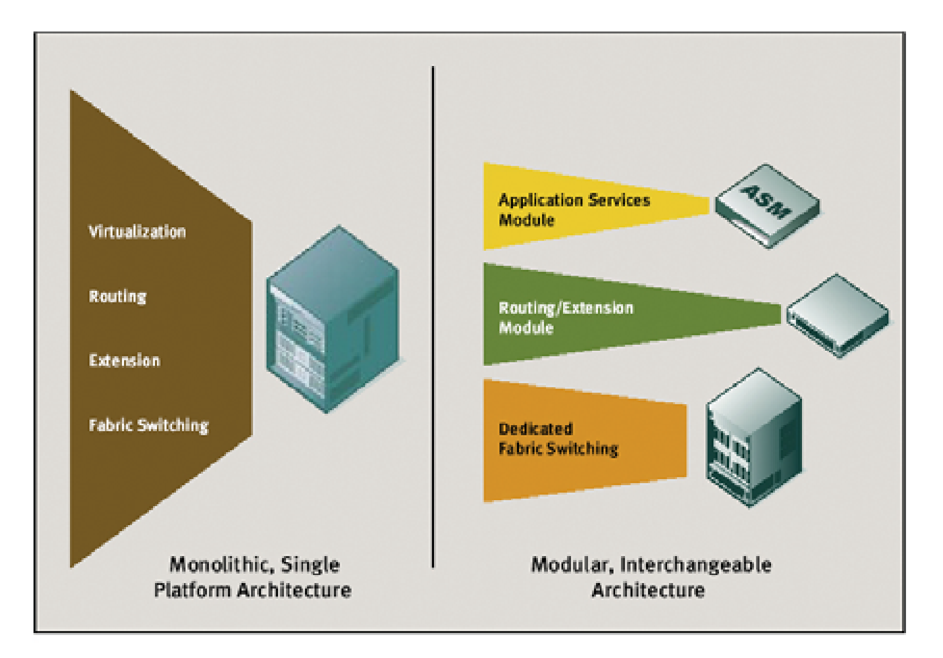
Existen, en términos generales, dos tipos de arquitectura de SAN: la monolítica y la modular. Como lo indica su nombre, la arquitectura monolítica trata de combinar los servicios avanzados dentro de la SAN tradicional, en una gran plataforma de hardware que forma parte de la capa de transporte (layer 2), incorporando un esquema de proveedor único, impidiendo el incremento independiente de las instalaciones.
Contrariamente, la arquitectura modular adhiere componentes que interactúan con la capa de



transporte básica (layer 2). De este modo, marca una clara diferencia entre esta última y los servicios avanzados. Al ser independientes los servicios de la capa 2 del resto de los servicios de otros niveles, se pueden sustituir los componentes sin que eso implique una renovación de toda la instalación de almacenamiento. Entre otros aspectos estratégicos, también se pueden incorporar servicios avanzados con total transparencia en la SAN existente y la administración del conjunto de recursos en forma simple.

Ventajas Competitivas de las Soluciones Modulares

Todas las organizaciones buscan obtener una ventaja competitiva y crecer en su mercado, al mismo tiempo de tener que cumplir con las regulaciones vigentes, enfrentando muchos de los mismos desafíos y problemas de almacenamiento de información que poseen las grandes empresas:
- El crecimiento de los datos continúa acelerándose, siendo a veces difícil estimar la velocidad de crecimiento de los mismos.
- Los dispositivos de almacenamiento económicos



no son confiables y tienen un desempeño insatisfactorio.
- Los recursos de TI no son fácilmente adaptables en función de las necesidades.
- La infraestructura de almacenamiento es difícil de administrar: discos internos de servidores o almacenamiento conectado a servidores pertenecientes a diferentes proveedores.
- Las ventanas de backup y restauración se están reduciendo.
- Los objetivos del tiempo de recuperación de desastres (disaster recovery) requieren la recuperación de las aplicaciones en horas o en sólo minutos.
- Las aplicaciones no cumplen con las expectativas de desempeño y disponibilidad.
- Los requisitos de cumplimiento de nuevas regulaciones vigentes y los temores de posibles litigios exigen que los datos se conserven en almacenamientos a prueba de manipulaciones durante períodos de tiempo definidos y que permitan el acceso rápido a la información cuando sea necesario.
- Es preciso que la información "vieja" esté en línea y que se pueda acceder a ella en poco tiempo (en general, en cuestión de segundos o de minutos).

Para poder resolver ésta problemática, se debe contar con una solución de almacenamiento modular de avanzada, que permita la configuración y administración desde un "visor único"; con una interfaz sencilla y gráfica, que posea además una arquitectura modular, funciones de virtualización de almacenamiento externo, particionamiento lógico y replicación universal, que reduzca el costo total de propiedad (TCO), simplificando todo el entorno de almacenamiento, y maximizando los recursos disponibles, permitiendo la implementación de una Plataforma de Almacenamiento Universal, con configuraciones de almacenamiento por niveles (Tiered Storage), que permiten almacenar información con múltiples requisitos de archivo y desempeño.

Este tipo de soluciones admiten generalmente el particionamiento de caché, poseen funciones avanzadas para mejorar la confiabilidad y la utilización para cargas de trabajo específicas de las aplicaciones, así como soporte para configuraciones NAS, SAN fibre channel y ISCSI, opción de discos SATA y fibre channel que permiten adaptar el costo del almacenamiento al valor de los datos, un sistema de administración de todo el almacenamiento desde "un solo visor", componentes redundantes que se pueden intercambiar sin detener el sistema, herramientas de servicio "call home" de mantenimiento remoto para garantizar la mayor disponibilidad, soporte para NAS y iSCSI, que permiten administrar los volúmenes basados en IP con las mismas herramientas que los volúmenes SAN, implementar aplicaciones de distribución (streaming) de información multimedia o video que requieren almacenamiento rentable y con elevada disponibilidad, escalar en la capacidad de almacenamiento sin modificaciones estructurales, etc.

Las redes SAN tienen un bajo costo de implementación y un alto ROIM (Return On Information Management)

Alineación entre aplicaciones e información

En la actualidad, existen varias opciones para diseñar una SAN que sea independiente de las plataformas de los servidores, para convertirlas en un servicio de la red. Las nuevas tecnologías que han surgido en los últimos años han permitido ampliar los servicios tradicionales, entre los que se pueden mencionar los de Storage Over IP, que tiene como funcionalidades la replicación de datos y extensión de la SAN a través de distancias prácticamente ilimitadas, y la conexión, a través del protocolo iSCSI, de servidores conectados a la SAN a través de Ethernet.

Estas soluciones, mediante diversas técnicas de virtualización, simplifican la administración, replicación y cualquier tipo de proceso en forma no disruptiva, característica imprescindible en las instalaciones de un Data Center.

Es fundamental, para garantizar estas funcionalidades, contar con un diseño modular del conjunto de la SAN, y con productos que permitan alinear la infraestructura de almacenamiento a las necesidades del negocio, aplicaciones y software en general.

Las redes modulares SAN permiten la centralización de datos, acelerar los tiempos de respuesta para todo tipo de proceso de información y una alta disponibilidad de la información administrada.

"Modular" Compuesto por distintas entidades, que pueden ser ordenadas y re-ordenadas en una configuración deseada.
Como quiera llamarse, en cualquier parte del mundo: moduler, modulieren, per modulare...
Como en los restaurantes, donde podemos elegir a la carta entre una amplia gama de platos, en tamaños y formas diferentes, con precios y calidades distintas; pensados para que el comensal haga sus propias combinaciones.

Los beneficios de contar con una red SAN

- Disponibilidad: La información es accesible para cualquier aplicación a través de múltiples rutas.
- Confiabilidad: El transporte seguro y confiable de los datos asegura una baja tasa de errores y la habilidad de recuperar la información en caso de fallas.
- Escalabilidad: Pueden incorporarse nuevos servidores y dispositivos de almacenamiento en forma independiente unos de otros.
- Performance: Altos anchos de banda para el transporte de información.
- Administración: La utilización de estándares y de software específicos permite una gestión centralizada y una detección y corrección proactiva de los errores.
- Retorno de la inversión en gestión de la información: Gracias al incremento de la redundancia y las mejoras en la administración de los datos, así como por la escalabilidad de las soluciones, las redes SAN tienen un bajo costo de implementación y un alto ROIM (Return On Information Management).





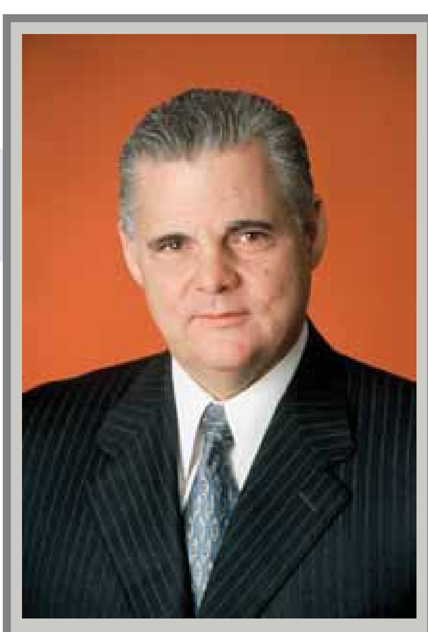
Nuestra Misión: Preservar la información de su empresa.

Joe Tucci, elegido como unos de los mejores CEOs de 2004 por la revista BusinessWeek. En cuatro años de trabajo en EMC, ha reactivado las ventas y el aumento de las utilidades y ha restablecido el liderazgo de la empresa en la industria del almacenamiento de información.

Los CEOs enfrentan hoy un tremendo desafío. La información y los requerimientos regulatorios crecen más rápido que sus presupuestos, al tiempo que deben encontrar mecanismos más eficientes para administrar y proteger su información, reducir costos y complejidades, obtener el máximo valor de sus activos de TI y cumplir con todas las normas de regulación legal. Todo esto - además- debe ser acompañado por un acceso más ágil a la información.

Ante esta situación, la respuesta de EMC ha sido convertirse en una compañía experta en ILM, es decir en una empresa para la Administración del Ciclo de Vida de la Información. Esta acción tiene como fin permitirles a nuestros clientes extraer el máximo valor de sus datos, al costo total más bajo, en cualquier momento. EMC es actualmente el único jugador del mercado de TI que puede ofrecer la tecnología y los servicios específicos que un cliente requiere para implementar desde cero una estrategia integral de ILM.

Este proceso comienza con la implementación de una red de almacenamiento. EMC continúa siendo la empresa que más invierte en la industria para ofrecer la más amplia oferta y variedad de storage. Tanto para la consolidación del almacenamiento de todos los servidores en un punto único (redes SAN) como para el almacenamiento conectado a la red con IP (NAS), los dispositivos de EMC cuentan con tecnología de canal de fibra y discos ATA que permiten a nuestros clientes elegir la alternativa más indicada en términos de funcionalidad, performance y costos.



Joe Tucci, Presidente y CEO de EMC, comenta la estrategia de la Corporación:

"La Administración del Ciclo de Vida de la Información: un valor para nuestros clientes, una oportunidad para EMC"



Adicionalmente -para aquellos clientes que requieren algo más que los procedimientos tradicionales de backup en cinta-, EMC cuenta con una oferta sin igual que satisface todos los niveles de protección y recuperación de las informaciones demandadas por las entidades que regulan los negocios en cualquier lugar del mundo. La adquisición de LEGATO, el año pasado, nos permite ofrecer software para backup e incluir sistemas de protección en nuestros dispositivos de storage, logrando así los máximos niveles de prevención ante pérdidas de información y un nivel de acceso superior a los datos.

El valor de la información se modifica constantemente. Los clientes demandan la posibilidad de migrar datos de manera dinámica a través de todas las plataformas instaladas, y poder brindar a sus organizaciones el mejor servicio, en el menor tiempo y al costo más bajo.

Tanto LEGATO como Documentum -otra empresa de software adquirida por EMC en 2003-, expanden nuestras posibilidades para brindar una prestación superior.

Gracias a Documentum logramos también dar un paso más: administrar la información no estructurada -como imágenes de cheques, planillas de cálculo, documentos, emails, videos digitales, radiografías, contenidos en formato Web- que constituye la mayor parte de los datos concebidos hoy en día. Documentum ubica todos estos contenidos en un repositorio único, donde la información puede ser guardada, autenticada y utilizada de la manera más dinámica durante todo su ciclo de vida.

El manejo integral de todos los activos de información a lo largo de toda la organización, constituye un elemento esencial para el ahorro de costos y la mejora en la productividad. Esto es lo que realmente destaca al software EMC Control Center, ya que otorga a los clientes una manera única de administrarlos.

Cada vez más, los clientes demandan un software que facilite el movimiento de la información y sus aplicaciones sin interrupciones en el negocio, mediante la conformación de un pool centralizado de almacenamiento y servidores. Atenta a esta necesidad, EMC adquirió VMware, empresa líder en software para virtualización. Toda esta oferta de software -LEGATO + Documentum + VMware- está disponible para nuestros partners a fin de que puedan integrarla a sus soluciones.

Sumados a esta oferta de excelencia en productos y tecnologías, los servicios profesionales de EMC nos permiten ser un proveedor total. Nuestros clientes poseen una oferta integral para la planificación, el diseño y la implementación de su estrategia de storage, con su posterior administración y soporte permanente. Este conjunto de soluciones cobra aún más valor gracias al aporte de nuestros socios de negocios: empresas tecnológicas líderes, proveedores de software independientes, integradores de sistemas y resellers.

ILM está acaparando la atención de nuestros clientes. Hacia allí está yendo la industria. Gracias a nuestro enorme diferencial en tecnología y a nuestro portfolio de servicios, desde EMC estamos liderando el camino. ■

EMC²
where information lives®

Almacenamiento, innovación y logros. Nacida en Massachussets, creció para permanecer y liderar.

- Una tradición permanente de innovación y crecimiento desde 1979.

- Uno de los 10 mayores vendors de tecnología de la información del mundo.

- El vendor N°1 de sistemas de almacenamiento por 7 años consecutivos.

- Una de las 5 más grandes empresas de software del mundo.

- Más de 2.000 patentes de productos aprobadas o en curso.

- Más del 90% de las empresas de Fortune 500 son clientes de EMC.

- Ayuda a los clientes a administrar su información en todo su ciclo de vida.

- Más de 21.000 empleados, 7.000 en Massachussets.

Microsoft TechNet



Windows® Storage Server es un servidor dedicado a entregar servicios de archivos e impresoras basado en Windows Server™ 2003. Este servidor esta diseñado para ofrecer confiabilidad, integración y el mejor precio/rendimiento. Windows® Storage Server se integra con la plataforma existente y soporta heterogéneos servicios de archivos, y también incluye los servicios de replicación y respaldo para la información almacenada. Además, Windows® Storage Server es una solución ideal para la consolidación de varios servidores de archivos que permite reducir los costos y administrar el almacenamiento de archivos basado en políticas.

Windows® Storage Server incluye características avanzadas que mejoran la disponibilidad, tales como las de respaldos tipo "Point in Time1", replicación y servicios de cluster. Windows® Storage Server es una solución "preconfigurada", la cual puede fácilmente ponerse en producción en pocos minutos. Asimismo, tiene una interfase WEB intuitiva de administración diseñada para facilitar la operación de los administradores. Las soluciones preconfiguradas de Windows® Storage Server son provistas a través de fabricantes de equipos (OEM2), las cuales consideran diferentes rangos y clientes finales. Estas pueden contener desde algunos gigabytes (GB) hasta varios terabytes de almacenamiento.

Windows® Storage Server provee acceso SCSI a través de Ethernet, protocolo denominado ISCSI, que permite acceder al servidor a través de un protocolo diseñado específicamente para la transferencia de datos. La ventaja de esta solución es que utiliza equipamiento Ethernet, considerablemente menos costoso que el Fiberchanel. Para la utilización de ISCSI se recomienda separar la red de clientes de la red de Datos, además, se pueden incorporar equipos Ethernet de Gigabit para mejorar la velocidad del acceso al almacenamiento.

Las tecnologías ISCSI se pueden utilizar en conjunto con el servicio de cluster de Windows Server Enterprise, para poner aplicaciones y servicios en modalidad de tolerancia a fallas. Los servicios y aplicaciones que se pueden utilizar son, por ejemplo: Carpetas e impresoras compartidas y Exchange Server (fig. 1).

Las características para el almacenamiento basado en políticas de Windows Server 2003 Release 2, también están disponibles en Windows® Storage Server, por ejemplo: Definición de cuotas a nivel de directorio y filtros para el almacenamiento de contenido.

Además, también podemos encontrar las nuevas funcionalidades del servicio distribuido de archivos, como es el caso del algoritmo de compresión diferencial remoto y el servicio de tolerancia a fallas de carpetas compartidas.

El servicio de cuotas se ha mejorado y se ofrecen dos características fundamentales. La primera característica es la definición de cuotas a nivel de volúmenes por usuario, la cual permite delimitar un espacio específico para un usurario en un volumen de un servidor. La segunda corresponde a la delimitación de un espacio específico a nivel de un directorio.

Fig 1.

El servicio de filtro de contenido permite a los administradores prohibir que los usuarios almacenen contenido indebido dentro de los servidores, por ejemplo, se pueden definir que no se puedan almacenar archivos tipo MP3, JPEG, WMA, etc..

El algoritmo de compresión diferencial remoto funciona en conjunto con el servicio de replicación de archivos. La ventaja fundamental es que este algoritmo detecta los cambios dentro de un archivo y solamente replica estos. Por ejemplo, antiguamente, si existía la replicación de un archivo Powerpoint de 10 Mb entre dos servidores y en uno de ellos se cambiaba solo el título de la presentación, el servicio de replicación sincronizaba los 10 Mb con el servidor remoto. Lo que sucede ahora con el nuevo algoritmo, es que este detecta los cambios correspondientes al titulo y solamente sincroniza estos cambios. Por lo tanto, la incorporación de esta nueva funcionalidad hace un uso más eficiente de los anchos de banda sobre todo en enlaces WAN.

El servicio distribuido de archivos permite colocar una carpeta compartida en alta disponibilidad, para el acceso de los usuarios. Esta característica permite independizar el nombre de los servidores del acceso a capetas compartidas, solo se define una raíz y esta puede estar almacenada en uno o varios servidores de respaldo. En conjunto con el servicio de replicación, se puede sincronizar en línea la información del servidor principal hacia el o los servidores de respaldo de manera tal que si el servidor que contiene la raíz sufre un desperfecto, uno servidores de respaldo automáticamente asumen esta función y continúan entregando el servicio a los clientes.

En resumen, Windows® Storage Server es ofrecido a través de una amplia red de socios de negocios y está diseñado para cubrir distintos escenarios orientados a almacenar y compartir archivos. Los usuarios pueden requerirlo para cubrir sus necesidades de almacenamiento NAS/SAN, respaldos, restauración, replicación y consolidación de servidores.

Para mayor información sobre este producto recomendamos acceder al siguiente link: *http://www.microsoft.com/windowsserversystem/wss2003/default.mspx*.

Allí encontrará información sobre las características del producto, principales beneficios, respuestas a preguntas frecuentes, información técnica del producto, y todo sobre los eventos de capacitación.

Si desea conocer más acerca de las funcionalidades y beneficios de Windows® Storage Server R2, le sugerimos acceder también, a un Webcast de Microsoft TechNet (en inglés) siguiendo el link: *http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032284687&EventCategory=4&culture=en-US&CountryCode=US*

[1] *Point in Time: Copias realizadas como fotografías de los datos (Snapshot) en un momento determinado.*
[2] *OEM: Other Equipment Manufacture.*

Almacenamiento y salud, una solución de IBM

El centro médico de la Universidad de Rochester pone los datos de los pacientes en la punta de los dedos de los profesionales médicos.

El Nuevo Sistema Archivo De Imagines y Comunicaciones (Picture Archiving And Communication System [PACS]), en el centro médico de la Universidad de Rochester (URMC) hace que la información vital sobre pacientes y sus tratamientos esté disponible al personal calificado a través de las extensas instalaciones del URMC.

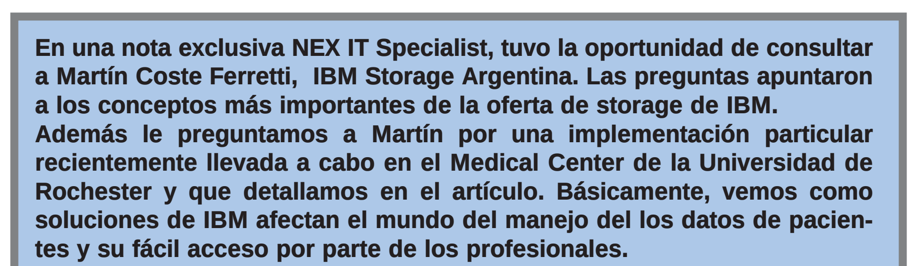
Necesidades de negocios
El URMC necesitaba una nueva solución PACS que integrara partes clave de los datos de los pacientes (incluyendo rayos X y otras imágenes) en historias clínicas virtuales, y darle al personal de médicos dispersos un acceso más rápido a esta información bajo demanda.

Retos Clave
A parte de permitir la adquisición, almacenamiento, entrega y muestreo de los registros médicos, la nueva solución tenía que ser robusta y lo suficientemente escalable para manejar la carga de trabajo de la URMC que se encuentra constantemente en aumento.

Solución: Servicios de Tecnología Integrada
El equipo de Servicios De Tecnología Integrada, (parte de los Servicios Globales de IBM), fue elegido para implementar sistemas de almacenamiento de IBM como soporte de la aplicación System 5 PACS de Kodak. Trabajando directamente con las especificaciones provistas por Kodak, el equipo de IBM instaló una solución de hardware certificado completa y proveyó todos los servicios necearlos para la implementación y testeo.
El equipo de IBM también integró la red de switches Cisco y componentes de storage area network (SAN) de la solución PACS, la cual corre en conjunto con hardware de Sun Microsystems y una base de datos Oracle. La capacidad total del nuevo sistema es de aproximadamente 75 terabytes para los tres sitios de almacenamiento principales y 120 terabytes para el sitio de backup.

Resultados
Hoy, doctores, enfermeras, técnicos de rayos X y otro personal, acceden rutinariamente al sistema PACS desde 73 estaciones de trabajo localizadas a lo largo y ancho del complejo URMC. La nueva solución muestra imágenes médicas, como rayos X y tomografías, junto con gráficos de los pacientes y e historias clínicas. Con una infraestructura de almacenamiento altamente escalable y confiable, soportando la aplicación PACS, el URMC se puede enfocar en entregar

Información de Clientes
El centro médico de la Universidad de Rochester es el punto central del conocimiento médico de vanguardia y experiencia para el centro de Nueva York, y la región de Finger Lake al Norte del Estado de Nueva York. Una institución de enseñanza e investigación, los recursos del URMC incluyen un centro de asistencia a pacientes que padecen quemaduras, epilépticos, a enfermos de hígado, y un centro de transplantes cardíacos como también instalaciones para otros servicios especializados. Con más de 470 investigadores, el URMC califica entre los primeros veinticinco de todos los centros médicos entre todos los que realizan investigación con subvenciones federales. Otra instalación de URMC incluye el Centro Dental Eastman, el Grupo Facultativo Médico de la Universidad de Rochester, el Strong Memorial Hospital y el Hospital de Niños Golisano en Strong.



En una nota exclusiva NEX IT Specialist, tuvo la oportunidad de consultar a Martín Coste Ferretti, IBM Storage Argentina. Las preguntas apuntaron a los conceptos más importantes de la oferta de storage de IBM. Además le preguntamos a Martín por una implementación particular recientemente llevada a cabo en el Medical Center de la Universidad de Rochester y que detallamos en el artículo. Básicamente, vemos como soluciones de IBM afectan el mundo del manejo del los datos de pacientes y su fácil acceso por parte de los profesionales.

NEX: *Es evidente que las últimas tendencias en storage buscan simplificar la infraestructura. ¿Qué conceptos aparecen en el mundo del storage?*
MC: *Las últimas tendencias en Storage están orientadas a simplificar y reducir costos. Es por esto, que en un entorno de crecimiento exponencial de datos e información a almacenar, es muy necesario tener una infraestructura simple, flexible, escalable y fácilmente administrable.*
Basada en esta necesidad IBM elabora y desarrolla sus conceptos de IT simplification, Virtualization, y Automatización.

NEX: *¿Qué es ILM?*
MC: *ILM (Information Life Cycle Managment) Según la SNIA (Storage Networking Industry Association) ILM es el compendio de políticas, procesos, prácticas y herramientas usadas para alinear el valor comercial de la información con la infraestructura de IT más apropiada y más efectiva en términos de funcionalidad y costos, desde que el dato es creado hasta su eliminación final. Llevado al cliente, la estrategia de ILM implementada correctamente le permitirá automatizar y optimizar sus políticas de "data placement", de manera de establecer jerarquías de almacenamiento asociadas a las necesidades de su negocio.*

NEX: *¿Cómo se relaciona una implementación de storage con la continuidad de los negocios?*
MC: *La implementación de una solución de storage debe ofrecer al negocio la continuidad de todos sus procesos.*
Dados los requerimientos actuales de operación 7x24, las soluciones actuales de almacenamiento ofrecen diferentes formas de minimizar el impacto de una salida de servicio.
Desde replicación sincrónica de datos a un sitio remoto, vaulting electrónico y replicación asincrónica, pasando por soluciones de virtualización de storage y Virtual Tape server.
Actualmente la tendencia más fuerte en el mercado es la de duplicar los datos a un sitio remoto y en este sentido las funciones de réplica remota de los sistemas de almacenamiento ofrecen capacidades especiales para atender este requerimiento del cliente; garantizando la consistencia y la accesibilidad de los datos en cuestión de segundos.

SEGURIDAD GRPS

Estás en una importante reunión de negocios, tu teléfono celular de última generación, entra en acción, y sin que te enteres, están gra-bando toda la conversación. Más tarde un hacker, recibe vía Internet todo el audio almacenado, y la reunión privada ya no lo es.

Pedro Paixao
Security Expert Manager, Check Point

Para una introducción a las tecnologías de comunicaciones móviles, ver el artículo de Ezequiel Pawelko publicado en la NEX IT Specialist #23, pág. 38.

Este es sin duda un escenario preocupante pero muy lejos de ser ciencia ficción. Los teléfonos celulares están convirtiéndose en puras plataformas de cómputo, con capacidades multimedia y de comunicación integradas. Pueden ejecutar código, y aplicaciones complejas, y prácticamente todos ellos ya soportan, de una manera u otra, email, chat, fotos, video, y web. Seguramente en un futuro no muy lejano, éstos irán reemplazando a las laptops como dispositivos de cómputo móviles por excelencia.
Al igual que otros dispositivos móviles, los celulares tienen su sistema operativo, sus aplicaciones, y claro sus vulnerabilidades. En junio de 2004 asistimos al nacimiento del Cabir, el primer gusano para teléfonos celulares, que se propaga vía Bluetooth. En febrero de 2005 el teléfono de Paris Hilton es atacado y le roban, fotos y videos personales, números de teléfono de otras celebridades, mensajes cortos SMS, así como notas de texto y otra información. En minutos todo esto estaba publicado en Internet siendo accesible a millones de personas en todo el mundo. Es una cuestión de tiempo para que escenarios como el inicialmente descripto se conviertan una realidad.
Desafortunadamente el problema no está solamente en los equipos terminales, los celulares. Para brindar servicios Internet siendo cada operadora tiene que instalar complejos sistemas de comunicación que ellos mismos son pasibles de ser atacados y a su vez comprometidos.
En un ataque más serio a redes móviles el hacker Nicolas Jacobsen se declaró culpable de las acusaciones de acceder a sistemas de cómputo de T-Mobile (operadora Americana) y durante más de un año poder leer correos, y otra información, de los más de 16 millones de usuarios de esa red, incluyendo los servicios secretos de los EE.UU.

GPRS

La mayoría de las operadoras brindan servicios de conectividad de datos vía GPRS, o General Packet Radio Service. El GPRS está basado en la infraestructura de comunicaciones GSM, y tiene como objetivos facilitar la utilización de servicios de datos basados en paquetes, mejorar, o eliminar el tiempo de conexión a la red, reducir costos de utilización de servicios de datos, y mejorar el ancho de banda disponible.
En una red GSM se multiplexan los canales de radio en 8 canales de tráfico de 14.4Kbps, que se mantienen alocados durante toda la duración de una llamada. Este método de comunicación, normalmente designado por conmutación de circuitos, o Circuit Switched en inglés, no es eficiente para aplicaciones basadas en paquetes de datos, que se comunican por ráfagas. Una mejor utilización de recursos pasa por liberar el canal de tráfico inmediatamente, siempre que no existan más datos para transmisión. Este método de comunicación es conocido como conmutación de paquetes, y es el utilizado en GPRS, permitiendo también una facturación mas amistosa para los usuarios, una vez que no es necesario cobrar las conexiones por tiempo, sino por cantidad de información. Otra de las ventajas es que el mismo canal de tráfico puede ser utilizado por varios usuarios a través una multiplexación estadística.
Para aumentar el ancho de banda disponible para datos, el GPRS puede hacer uso de varios canales de tráfico en simultáneo, siempre que la operadora lo permita y se requieran más recursos de la red. Paquetes de datos pueden ser directamente encaminados entre móviles y redes fijas, sobre TCP/IP o X25.
En la Figura 1 podemos ver la utilización, y optimización, que el GPRS hace de los canales de tráfico GSM, y verificar que el GPRS no añade ancho de banda al servicio GSM, antes comparte con este los recursos disponibles en cada momento. (Fig.1)

Arquitectura del Sistema GSM/GPRS

La Figura 2 enseña la arquitectura de una red GSM/GPRS en sus componente esenciales. Una celda es formada por el área de radio cubierta por una Base Station (BS) también conocida como Base Transciever Station (BTS). Un conjunto de varias BTSs es controlado por un Base Station Controller (BSC), y el grupo de BTSs, más el BSC se llama de Base Station Subsystem (BSS). El tráfico combinado de los móviles en sus res-

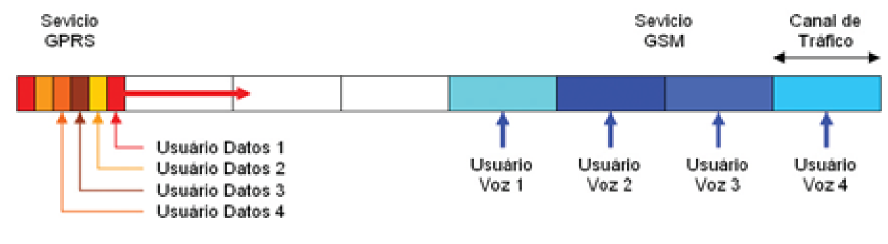


Fig.1 Utilización de Canales GSM por parte del GPRS

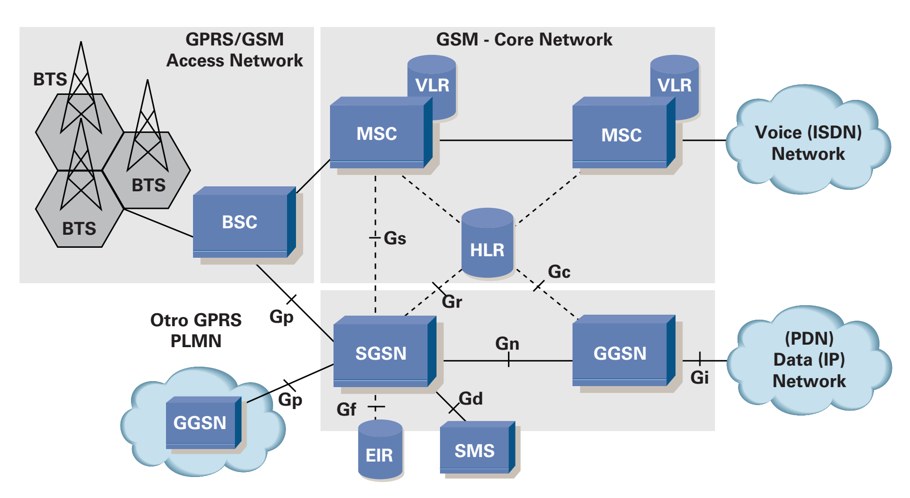


Fig.2 Arquitectura de la red GMS/GPRS

pectivas celdas es encaminado hacia el "cerebro" de la red, o el Mobile Switching Center (MSC). El MSC se encarga de hacer la conmutación de llamadas, interfaz con otras redes móviles o fijas, y también como mantenerse informado de la ubicación del móvil en la red. El MSC solo procesa llamadas de voz.

En el MSC existen varias bases de datos que son utilizadas para el control de llamadas y administración de red. Entre ellas están el Home Location Register (HLR), el Visitor Location Register (VLR), y el Equipment Identity Register (EIR). El HLR almacena toda la información permanente de cada suscriptor de la red, y también alguna información temporal como su ubicación. El VLR es responsable por un conjunto de BSSs que forman una Location Area (LA) y almacena los datos de los suscriptores que se encuentran es su área de responsabilidad. Esto incluye datos que fueron copiados del HLR para acceso más rápido, y otra información temporal que solo es relevante en su área local. El EIR almacena datos sobre los equipos móviles y es normalmente utilizado para combatir fraudes, manteniendo, por ejemplo, el listado de equipos clonados.

En GSM se distingue usuario y equipo terminal (teléfono) explícitamente. Además del número de teléfono, y serial del equipo terminal, existen otros identificadores, o direcciones, que son utilizados para administración de ubicación, o direccionamiento de otros elementos de red.

Así tenemos el International Mobile Station Equipment Identity (IMEI), que es como el número serial del terminal, y es único a nivel mundial. El IMEI es colocado en cada teléfono por el fabricante, y normalmente puede ser cambiado por software, por lo que no es muy utilizado en mecanismos de seguridad. Cada suscriptor de la red es identificado por International Mobile Subscriber Identity (IMSI) que es almacenado en el smart card, o Susbscriber Identity Module (SIM) del teléfono. El IMSI es como el serial del SIM, y es creado por la operadora del móvil, no por el fabricante. El IMSI no puede ser cambiado por el usuario por lo que puede ser utilizado para mecanismos de seguridad. En GSM, un terminal móvil solo puede ser utilizado si un SIM con un IMSI válido es introducido, en un equipo con un IMEI también valido. El número de teléfono real, o el Mobile Subcriber ISDN (MSISDN) es atribuido a cada suscriptor y almacenado en el SIM.

La integración de los servicios GPRS a la red GSM requiere el upgrade de algunos elementos existentes, como el HLR y VLR así como la introducción de dos nuevos elementos que se llaman de GPRS Support Nodes (GSN). El Serving GPRS Support Node (SGSN) es responsable por la entrega de paquetes a los móviles en su área de servicio, haciendo ruteo de paquetes, registro y ubicación. Se encarga también de hacer el handoff a otro SGSN cuando el móvil sale de su área de cobertura y entra en el área de otro SGSN.

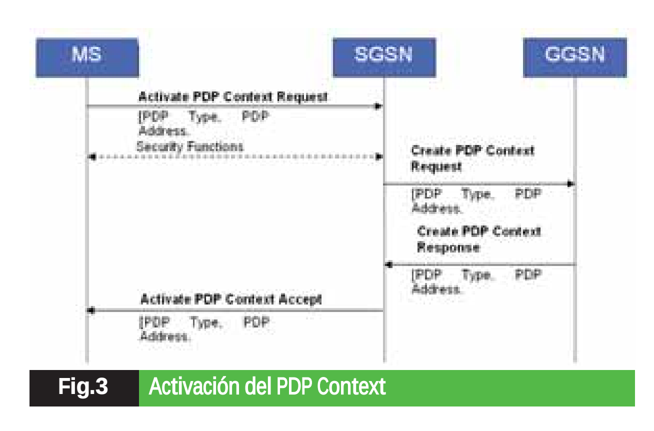


Fig.3 Activación del PDP Context

El Gateway GPRS Support Node (GGSN) es la interfaz entre la red GPRS y las redes de datos externas, convirtiendo los paquetes que provienen del SGSN en el formato de protocolo apropiado a la red con la cual el usuario desea comunicarse. Otra responsabilidad del GGSN es la facturación de servicios al usuario.

Por lo general un GGSN puede ser la puerta a otras redes, de varios SGSNs y cada SGSN puede enviar paquetes a varios GGSNs dependiente de la aplicación que se desee utilizar.

La comunicación entre SGSNs y GGSNs es totalmente basada en TCP/IP utilizando el GPRS Tunneling Protocol (GTP) y el backbone que los interconecta es una red IP. Por cuestiones de seguridad no deben existir protocolos no IP en el backbone GPRS.

En la Figura 2 podemos ver también las varias interfaces que interconectan los varios elementos y los más importantes para nuestra discusión son:

- Gb - Conecta el BSC con SGSN
- Gn - Conecta SGSNs y GGSNs en la misma red
- Gp - Conecta SGSNs y GGSNs en redes distintas (socios de roaming)
- Gf - Para consultas durante el período de registro para evitar fraudes
- Gi - Conecta la red móvil a redes de paquetes externas (Internet u otras)

Administración de Sesiones

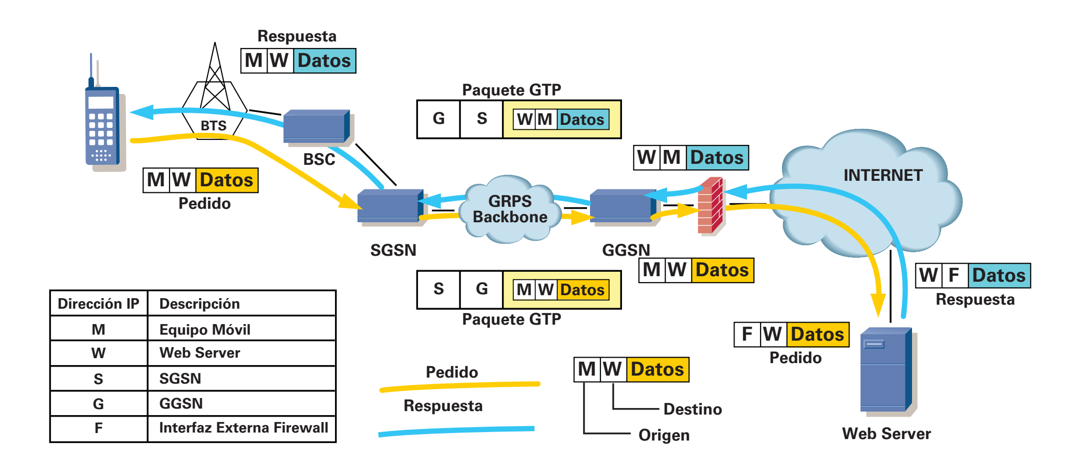
Antes que un móvil pueda utilizar los servicios de la red GPRS éste tiene que conectarse y registrarse en la red. A este proceso se llama "attach". Durante la fase de attach la red verifica la identidad del usuario (autenticación), verificando enseguida si este puede utilizar los servicios GPRS (autorización). Finalmente se copia la información del HLR para el SGSN y se atribuye un IMSI temporal (P-TMSI).

El proceso reverso se llama de "detach" y puede ser iniciado por el móvil o por la red (SGSN, o HLR.)

Después del attach, y antes de poder comunicarse con redes externas (Packet Data Networks), el móvil tiene que pedir una dirección de la red. A esta dirección se llama un Packet Data Protocol address o PDP address, que normalmente va ser una dirección IP; sin embargo el GPRS soporta también el X25. Para garantizar que los paquetes sean encaminados apropiadamente, los GSNs (SGSN y GGSN) y el móvil, tienen que almacenar todas las características de cada sesión. Ésto se hace creando un contexto de sesión que se llama de PDP Context. El PDP Context contiene información como el tipo (ejemplo IPv4), el PDP address (ejemplo 10.1.120.3), la calidad de servicio requerida, la dirección IP del SGSN y GGSN que soportan la sesión, etc. Después que se crea el PDP context y la sesión está activa, el móvil es visible en la PDN externa (ejemplo Internet).



Fig.4 Estructura de un paquete GTP



Dirección IP	Descripción
M	Equipo Móvil
W	Web Server
S	SGSN
G	GGSN
F	Interfaz Externa Firewall

Fig.5 Routing en Redes GPRS

GPRS Tunneling Protocol (GTP)

La comunicación entre SGSN y GGSN se hace exclusivamente en GTP y ningún otro sistema en la red debe utilizarlo o conocer su existencia. Él es transparente para los móviles y las PDNs, es como si el móvil estuviera directamente conectado con la red externa sin enterarse que es el GTP el que transporta sus datos entre GSNs. El GTP es un protocolo complejo y su descripción completa está fuera del los objetivos de este artículo.

Routing en GPRS

En la Figura 5 podemos ver como se hace el routing de paquetes en redes GPRS. Después del attach y la creación de la sesión GPRS y su PDP context, el móvil está listo para comunicarse con servidores externos. Cuando el usuario del móvil 'M' intenta ver una pagina del servidor web 'W', se genera un paquete HTTP que es enviado al SGSN 'S', que encapsula el pedido original dentro de un paquete GTP, y lo envía al GGSN 'G' que brinda servicios de conectividad web hacia Internet. El GGSN 'G' desempaqueta el GTP, retira el pedido original del móvil y lo encamina hacia el firewall 'F' de salida hacia Internet. El firewall 'F' hace una traducción de direcciones, y envía el paquete traducido al servidor web 'W'. El servidor, después de procesar el pedido, forma la respuesta y la envía de vuelta a 'F', luego el proceso se invierte.

Problemas de Seguridad

En su concepción el GPRS presenta varios problemas de seguridad que son evidentes, y pueden ser explotados para abusar de la red, de sus usuarios, no pagar por servicios, causar facturación excesiva a suscriptores, entre otros.

Como vimos en las secciones anteriores, el GPRS tiene muchos y complejos componentes que son implementados utilizando hardware y sistemas operacionales comunes. También se discutió que la comunicación entre muchos de estos sistemas, en el backbone GPRS, se hace con TCP/IP. Podemos entonces concluir que todas las vulnerabilidades y ataques conocidos del mundo Internet y sus servicios, se aplican directamente a estos elementos del GPRS.

Por otro lado las implementaciones de SGSNs y GGSNs no son tan maduras como el demás software utilizado en Internet, que ha estado bajo escrutinio contínuo durante años. Estas aplicaciones sufren de los mismos problemas de seguridad a que ya nos acostumbramos, como buffer overflows, ataques de denial of service, virus y gusanos. Debido a la interfaz de usuario limitada de los terminales móviles GPRS, algunos de estos ataques son de difícil ejecución pero no imposibles. En mayo del 2003 se confirmó el primer ataque de DoS contra un GGSN proveniente de un móvil. En esta instancia era posible parar el GGSN por completo, causando un reboot de la máquina, y con ello la completa disrupción de servicio a todos los suscriptores de la red que utilizaban dicho GGSN.

Otro ataque ya implementado se conoce con el nombre de Overbilling, o facturación excesiva. En una versión de este ataque, el hacker, utilizando un móvil GPRS conectado a una operadora, genera pedidos UDP hacia un servidor malicioso en Internet, que empieza a contestarle continuamente. Después el hacker desconecta su móvil liberando la dirección IP, o PDP Address que utilizó en la preparación del ataque. Un nuevo suscriptor, la víctima, se conecta a la red GPRS y recibe la dirección IP que pertenecía al hacker. Como el servidor malicioso en Internet sigue enviando paquetes UDP hacia esta dirección, le será facturado al usuario el uso de un servicio que éste no desea utilizar, y ni siquiera debería recibir. Esto no es un ataque de seguridad per se, pero permite al hacker causar graves problemas a la operadora y sus usuarios, que ven su factura crecer sin explicación aparente.

Uno de los problemas más graves de las redes GPRS es que el SGSN y GGSN confían uno en el otro, y no hay mecanismos de seguridad entre ellos. Por otra parte hay muy poca segmentación del backbone GPRS, redes de administración y enlaces con partners de roaming.

Un hacker podría conectarse a la operadora, obtener la dirección IP del GGSN al cual está conectado y, vía la interfaz Gi, intentar obtener la dirección IP de otros GGSNs, que le permitan utilizar otros servicios no disponibles en su plan, o no pagar por la utilización de estos servicios.

Este método, combinado con otros ataques que pueden hacerse contra implementaciones de GGSNs actuales, como la generación de paquetes GTP dentro de GTP, abren la puerta a ataques muy sofisticados, dentro de la red GPRS, en el caso en que un único GGSN sea comprometido. Este tipo de ataque se agranda cuando tenemos en cuenta socios de roaming. Hoy día, raras son las operadoras que implementan sistemas de seguridad sobre GTP, en el interfaz Gp. Esto significa que un GGSN comprometido en una operadora remota con la cual se tenga un acuerdo de roaming, permite atacar directamente el backbone de la operadora local. O sea la seguridad de la operadora local depende de la seguridad de un sin fin de otras empresas en todo el mundo! Esto es posible aún cuando existen firewalls tradicionales en las interfaces Gp, pues todo el tráfico entre GSNs se hace dentro del GTP, que para un firewall tradicional es un simple servicio UDP. Si no se utilizan firewalls capaces de "abrir" e inspeccionar el GTP es posible comprar el interfaz Gp con un enlace Internet sin protección alguna.

Podemos entonces decir que los ataques sobre GPRS se dividen en tres categorías:

- Anomalías del Protocolo GTP. Este tipo de ataques buscan impactar malas implementaciones de GSNs utilizando paquetes malformados que no cumplen con los estándares y como tal, jamás deberían ser utilizados en una red en buen funcionamiento.
- Ataques de Infraestructura. Estos ataques buscan obtener acceso a sistemas restringidos de la red, como por ejemplo, GSNs u otros sistemas de administración.
- Denegación de Servicios. Estos ataques intentar agotar los recursos existentes en la red para evitar que se puedan atender otros usuarios. Por ejemplo generar miles PDP Context activations hacia un SGSN.

El impacto de estos ataques puede ser muy grande, como es el ejemplo de GTP spoofing, que falsifica direcciones IP de sistemas en el backbone GPRS, o el GTP Attack Tunneling que encapsula ataques comunes de Internet en paquetes GTP, enviándolos contra el SGSN o GGSN.

Como siempre se diseñaron protocolos y estándares que no tienen en su base la seguridad, y en este momento la puerta está abierta para que un hacker cause disrupciones de servicio, robe información de otros suscritores, o envíe software directamente para otros móviles, vía Chat o otra aplicación, que le permiten el completo control de esos dispositivos. Cabe a las operadoras segmentar apropiadamente sus redes, instalar sistemas de seguridad GTP, y a nosotros, los usuarios, nos cabe la constante atención a nuestra factura de teléfono, así también como las aplicaciones que se encuentran en él instaladas. La próxima vez que compres un teléfono celular, éste ya va a hacer tantas cosas que seguramente vas a decir: Mirá mi teléfono también hace llamadas! ■



El Negocio del Software y Servicios Informáticos

Sergio Candelo
Director de Operaciones, Snoop Consulting

Para dar contexto al medioambiente en que nos movemos, me gustaría describir brevemente el mercado del SOFTWARE.

La actividad económica de servicios informáticos, como todo negocio, tiene sus particularidades. Hoy en nuestro país se lo considera una actividad industrial por ley nacional. Independientemente de si es o no industria, el SOFTWARE como actividad empresarial tiene sus características propias. Sobre este punto en particular, quiero ser mas preciso y realizar un pequeño análisis del mercado de SOFTWARE y de las actividades que dentro de ese mercado realiza Snoop Consulting.

¿Qué es el SOFTWARE? El SOFTWARE es algo intangible, etéreo, que nos permite acumular conocimiento, generar actividades, desarrollar ideas, llevar adelante industrias, empresas. Es una herramienta de apoyo a todas las actividades de hoy en día. Es impensable plantear cualquier actividad industrial sin un sistema de información. Es más, ya forma parte de nuestra vida cotidiana. Lo tenemos dentro del celular, Internet, etc. etc.

Dentro de este marco, encontramos empresas que se dedican al desarrollo de productos (que son SOFTWARE). Entre ellas tenemos una amplio abanico, desde la confección de SOFTWARE de base, Sistemas Operativos, Bases de Datos, Servidores de Aplicaciones, etc. etc., pasando por las que producen aplicaciones para distintas áreas generales de la empresa como ser los ERP, CRM, SMP, etc.; las que generan aplicaciones de uso domestico o de oficina, como procesadores de texto, planillas de cálculo, presentaciones, gestión de proyectos, etc. etc. así como también empresas que se dedican a realizar aplicaciones de nicho o de mercados muy particulares, por ejemplo, reserva de pasajes aéreos, extracción de petróleo, logística de diversas industrias, etc. etc. Otros realizan video juegos. Otros editores de imagen. Otros aplicaciones para cine y televisión.

Es decir hay una parte del mercado de SOFTWARE que es productora de "enlatados". Su estrategia comercial es la venta de las "cajas" y su estructura productiva se centra en generar aplicaciones y luego mejorar el SOFTWARE, que no tenga bugs, sacar nuevas versiones, actualizarlo tecnológicamente. Es decir, hay un área productiva que desarrolla el producto y un área comercial que lo vende.



El objetivo de este artículo es presentar la experiencia vivida por los socios de un emprendimiento que consistió en montar una consultora de sistemas.

Dependiendo la complejidad de la aplicación y de la utilización, el proceso de venta del SOFTWARE pude ser algo transaccional (que se compre en una tienda o un supermercado) a un proceso de venta consultiva que lleve más de 6 meses.

La otra pata del mercado de SOFTWARE esta en los servicios que ofrecen empresas para ayudar a utilizar la tecnología en el resto de las industrias. Aquí entran en juego las consultoras de IT. Dentro de este segmento se abre otro abanico de posibilidades de servicios ofrecidos, desde la provisión de RRHH a las áreas de sistemas de las distintas industrias, al manejo de proyectos y desarrollos de aplicaciones específicos para atender una necesidad puntual, capacitación, administración de la infraestructura de base, outsourcing, soporte de aplicaciones, soporte de infraestructura, soporte en tecnología, etc. etc.

El último componente del mercado de SOFTWARE y SI son las áreas de sistemas de todas las empresas de todas las industrias. Este sector también es demandante de recursos y en muchísimas ocasiones son generadores de aplicaciones propias y realizan todo los servicios mencionados en el párrafo anterior.

Resumiendo, el mercado de SOFTWARE consta de 3 actores claramente identificados, los que producen enlatados, los que ofrecen servicios, y las áreas de sistemas de todas las empresas y organizaciones que operan en la economía. Dentro de estos 3 grupos, Snoop Consulting forma parte del segundo. Y dentro de este hay una variedad y diversidad de mercados, servicios, clientes, soluciones, formas de contratación. En definitiva todos estamos en el mismo mercado y vivimos de alguna manera u otra.

Reseña Histórica

Snoop Consulting es una empresa de capitales nacionales constituida por 5 socios. Originalmente éramos 4 y luego, al año de fundada la compañía, se agregó el quinto.

Tres profesionales informáticos comenzaron a dar forma al nuevo emprendimiento. La idea de qué tipo de empresa, el mercado a atacar y el posicionamiento fue algo que se venía pensando desde dos años atrás a su fundación. Luego, al momento de lanzar la empresa, se incorpora el 4to socio, una persona que no venia del área de IT, sino de la economía.

Snoop Consulting nació el primero de agosto de 2000. Se inició con una misión, un objetivo. Cabe mencionar que la empresa se crea sin contar un negocio puntual o un contrato con un cliente de largo plazo, sino que se salió a buscar los clientes y los proyectos. Los socios dejamos nuestras actividades para dedicarnos de lleno a la creación y expansión de Snoop Consulting. Luego de seis meses de actividad ya contábamos con un pequeño pero nutrido grupo de clientes.

Objetivos iniciales

Nuestra Misión: *Simplificar el acceso de las empresas a tecnologías emergentes, que mejoren la productividad del negocio.*

La misión de Snoop es lograr la adopción de las tecnologías emergentes en los procesos tecnológicos de las empresas que ayuden al negocio que se dedican. La idea es convertirnos en agentes que transforman el invento en innovación. ¿Qué significa ésto? Cuando se crea algo nuevo no es fácil ni simple que se adopte. Tomemos como ejemplo la lamparita eléctrica. Desde su invención hasta que realmente se la utilizó en todas sus posibles aplicaciones (hoy en día se sigue utilizando) pasaron varios años. La idea de Snoop Consulting es justamente tomar los nuevos lenguajes, framework, etc. y utilizarlos en el desarrollo de aplicaciones concretas que se empleen para llevar adelante el negocio de la compañía.

Desde este punto de vista, Snoop Consulting se posicionó en Java en el 2000. Dado el conocimiento y la experiencia en objetos, y la visión de que sería una tecnología de punta, por un lado, y el conocimiento sobre las herramientas de Oracle por el otro, junto con la expectativa de una migración de Oracle desde tecnologías propietarias hacia tecnologías abiertas y Java como plataforma, se analizó que iba a existir una necesidad puntal de servicios de consultoría para acercar al mundo Oracle la tecnología Java. Es decir tratamos de acercar el invento a la innovación.

La visión de que Java sería una tecnología a ser utilizada masivamente, fue confirmada por el éxito de la misma ya que en estos momentos es la tecnología adoptada por la gran mayoría de empresas para el desarrollo de aplicaciones críticas. Como todo en la vida, además de prepararse hay que tener suerte. Snoop Consulting eligió Java y el tiempo le dio la razón.

Hoy en día nuestro foco se encuentra en

- SOA (Service Oriented Architecture)
- Desarrollo con tecnologías J2EE y .NET
- Bases de Datos y Misión Crítica
- Investigación y desarrollo en Data Mining, Information Retrieval y MDA (Model-Driven Architecture).

Manteniendo en todos estos frentes vigente la misión de la compañía.

Plan de negocios y de marketing

Snoop Consulting se planta inicialmente con la idea sólida de trabajar en tecnología de base Oracle y plataforma de desarrollo JAVA y sobre ella surgen todos los servicios que pueden ser ofrecidos: infraestructura, capacitación, instalaciones, soporte, inclusión de mejoras. Por ejemplo cuando aparece la Alta Disponibilidad en Bases de Datos (Real Application Cluster en Oracle), Snoop Consulting es el primer partner de Oracle de la región en implementarlo.

Iniciarse en el mercado no es una tarea sencilla. Si bien éramos concientes de nuestro nivel técnico, conseguir clientes donde demostrarlo fue muy difícil. Como dice el refrán, "no solo serlo sino parecerlo".

Los servicios prestados por Snoop Consulting son demandados por las áreas de sistemas de las empresas. Esta situación determina claramente que nuestros clientes potenciales sean empresas de medianas a grandes.

Ante esta situación, la introducción de Snoop Consulting al mercado fue a través del relacionamiento con partners tecnológicos. Por ejemplo, el posicionarnos dentro de Oracle nos permitió brindar servicios de capacitación y transferencia de tecnología a muchos de los partners de este ven-

dor. Este punto lo desarrollaremos con mayor profundidad más adelante.
Actualmente los servicios que brindamos son más amplios, y entre ellos podemos mencionar:

- *Desarrollo de proyectos con tecnologías J2EE y .NET (Análisis/Diseño/Implementación)*
- *Consultoría tecnológica*
- *High Performance Computing*
- *Seguridad y auditoria de sistemas*
- *Sistemas de Misión Crítica*
- *Tuning de sistemas*
- *Data Mining*
- *Usabilidad*
- *Capacitación en productos, procedimientos y metodologías*
- *Mentoring y Coaching*
- *Prevención y soporte ante contingencias*

Adicionalmente realizamos ventas de licencias de SOFTWARE enlatado, no siendo esta una actividad principal de Snoop.
Con el paso del tiempo, una vez demostrada nuestra calidad de trabajo y el propio crecimiento de Snoop Consulting, se fue modificando nuestra forma de venta de indirecta (a través de partners) a directa, atendiendo nosotros mismos a los clientes. Para dar un orden de magnitud a este párrafo, podemos decir que en el primer año, la facturación de Snoop Consulting se distribuía en 15% venta directa y 85% venta indirecta, guarismos que se han invertido en los últimos años.
Hacia fines de 2002, la estrategia de Snoop Consulting fue posicionarse claramente como proveedor de soluciones SOA (Software Oriented Architecture) lo que determinó una apertura hacia otros vendors además de Oracle. En el transcurso de 2004 nos posicionamos fuertemente en todas las tecnologías y en el 2005 comenzamos más fuertemente la tarea de Partnerships y Alianzas.

Partnerships

- ORACLE - Certified Advantage Partner
- BM
- BEA

Alianzas

- Microsoft
- SAP
- Dell
- Hewlet Packard
- Red Hat Linux

Cómo se eligió el equipo fundacional y su importancia

El equipo fundacional fueron los socios. Técnicamente de muy buen nivel. Adicionalmente se instrumentó un esquema para la búsqueda y selección de recursos con muy buenos resultados, demostrado en que los primeros 10 empleados aun hoy continúen en la compañía y en su gran mayoría llevando adelante tareas claves.

Los negocios tienen dos aristas: relaciones y confianza

Por un lado, contamos con un socio con habilidades innatas, que genera rápidamente confianza y establece relaciones duraderas. Estas cualidades, de todas formas, no disminuyen la capacidad técnica. Realmente la combinación de estas dos características permitió que Snoop Consulting tuviera una rápida aceptación. Era menos difícil que un cliente nos pruebe, pero obviamente, que esta posibilidad debía respaldarse con resultados concretos y positivos. Aquí se conjugaba la experiencia tecnología y el aspecto comercial. Esto fue nuestra punta de lanza para ingresar al mercado de Software y Servicios Informáticos.
Por otro lado se necesitaba una sólida estructura de conocimiento para poder llevar adelante la misión de Snoop Consulting. No es trivial ser un partner tecnológico que domine la tecnología de punta. Eso se logra sólo con recursos fuertemente capacitados. En esta línea, los socios de Snoop Consulting permitían contar con esta seguridad en el área técnica. Adicionalmente se realizó un reclutamiento de recursos con foco en la "madera". Una vez que se tenía esta base, la capacitación fue una constante. Así, pudo construirse una pirámide de conocimientos que nos permitieron tomar más proyectos con buenos resultados.
De alguna manera, los socios de Snoop Consulting siempre fuimos muy inquietos en temas de investigación. La misión de Snoop Consulting lleva impregnado este sello. Obviamente, los recursos seleccionados, siempre tienen que tener un "algo" de innovación y deseos de mejorarse.
Una pequeña digresión. En el campo de la informática, el estar actualizado e informado de los nuevos lenguajes, sistemas y procesos, es más una necesidad de mantener el capital humano de cada recurso que una vocación por la investigación. Es una manera de no volverse obsoleto. El mercado tecnológico avanza a una rapidez que no permite establecerse en una tecnología y descansar. El "consigue los laureles y échate a dormir" no aplica en este contexto por un periodo prolongado de tiempo. Es posible que los "javólogos" de hoy sean, en un futuro no muy lejano, los coboleros del mañana.
En resumen, una buena gestión comercial con excelente nivel de preventas, y un equipo sólido debajo para lograr resultados garantizados, fue la estrategia de marketing más importante en los primeros años. Los primeros proyectos donde demostrar solvencia y conocimiento eran claves para el devenir de la compañía. Los primeros casos de éxito tienen una trascendencia elevada. La recomendación de boca en boca es la mejor campaña de marketing al inicio.
Una vez afianzados en el mercado, la política de Marketing ha sido muy fuerte. Se logró centralizar la comunicación en los espacios y sectores específicos de nuestros servicios. Inicialmente fueron charlas y seminarios, luego participando en eventos hasta terminar organizando un seminario para desarrolladores en la primavera pasada con una asistencia de mas de 1200 personas y el sponsoreo de los principales vendors y asociaciones del mercado informático argentino.

Asociatividad y Networking

Los servicios ofrecidos por Snoop Consulting, desde los inicios y hasta nuestros días, son servicios solicitados por las áreas de sistemas. Por lo tanto los clientes potenciales son empresas que en primer lugar contengan en sus estructuras áreas de sistemas. Empresas con áreas de sistemas naturalmente no son micro-emprendimientos, sino empresas grandes con estructuras, departamentos, jerarquías, etc. etc. Por lo tanto naturalmente los clientes de Snoop Consulting son empresas de medianas a grandes, y principalmente grandes.

Las top 500 de argentina son el cliente objetivo de Snoop Consulting.

Siguiendo con el ejemplo de Alta Disponibilidad en Bases de Datos, no cualquier empresa necesita tener los sistemas con alta disponibilidad y fácilmente escalables. Realmente la importancia del negocio tiene que ser tal que destinen a sistemas un monto inferior a la mejora en el negocio que este genera. Un ejemplo, si una empresa decide desarrollar una aplicación para mejorar algún área de su negocio e invierte 1 millón de pesos, la lógica económica nos indica que esa aplicación deberá mejorar el área mencionada y con esa eficiencia obtener mucho más que el millón invertido.
En este contexto no es simple ingresar al mercado tecnológico de las grandes empresas de Argentina siendo una pyme (pequeñísima en los orígenes) que recién inicia sus actividades. Simplemente, muchas empresas grandes argentinas solicitan una historia financiera, patrimonial y de casos de éxito que no logra hacerse en un par de semanas de actividad.
Con esto en mente la estrategia de Snoop fue complementarse con consultoras medianas o grandes y con vendors de SOFTWARE donde el expertise de Snoop, por ser de nicho, no competía con sus servicios. Es decir se logró una muy buena relación de "socios tecnológicos". Como muestra de este desempeño, Oracle nos premio como mejor partner de networking tecnológico en el primer año de trabajo en conjunto.
El primer año de Snoop Consulting mostró que más del 70% de nuestra facturación fuera realizada a empresas de servicios tecnológicos.
El crecimiento de la compañía y los casos de éxito hicieron que mejore nuestra performance. No obstante nuestra manera de trabajar como "socios" con otras empresa de tecnología nunca fue dado de baja. Si bien en 2005 la proporción de la facturación directa (a Clientes propios) de Snoop Consulting creció a más del 85%, la cantidad de empresas tecnológicas con las que trabajamos siguió creciendo, tanto en cantidad como en valor absoluto.

"Necesito mantener
la información segura,
en todo lugar."

"Necesito ayudar
a mis pacientes,
desde cualquier lugar."

Check Point Connectra hace feliz a ambos con acceso desde cualquier lugar y seguridad en todo lugar.

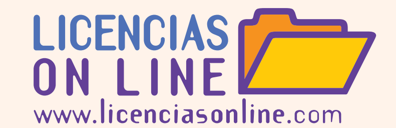
NGX

Mantener la información segura no tiene porque estar en contraposición con proveer acceso sencillo. Solo Check Point Connectra combina acceso SSL VPN desde cualquier Web-browser, asegura la transmisión de información sobre salud via SSL, y provee la inmunidad más potente contra spyware, gusanos y otros riesgos a la privacidad de datos.

Connectra es la receta correcta para acceso desde cualquier lugar y seguridad en todo lugar.

Conéctate hoy a www.licenciasonline.com para información sobre soluciones Connectra en salud.

Aprenda como usted puede hacer que los médicos estén contentos mientras mantiene la información segura a través del acceso remoto disponible más seguro y conveniente. Y descubra como Connectra provee los controles de seguridad que usted necesita de modo que pueda cumplir las regulaciones de HIPPA.





Cómo se superaron las crisis externas e internas

No todo es color de rosas. Snoop Consulting a los 16 meses de vida se encontró con la peor crisis económica argentina de los últimos tiempos. Si bien la hecatombe ocurrió en diciembre de 2001, los cambios de ministros y la situación coyuntural no eran buenos desde 1998, momento en que el país había comenzado su fase de decrecimiento.

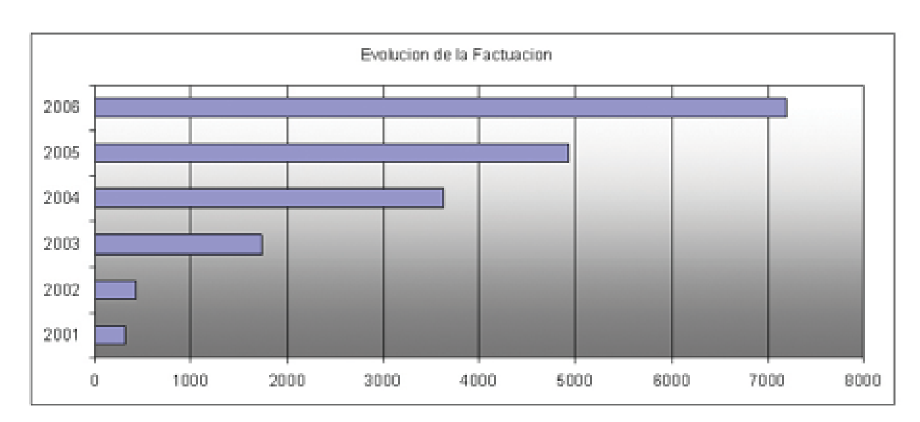
La manera de superar esta crisis externa fue por un lado ofrecer servicios que mejoraban la utilización de la capacidad tecnología actual al máximo potencial. Los usuarios de Office generalmente no sabemos cual es el potencial de un programa y toda la funcionalidad que tiene. En las áreas de sistemas ocurre algo similar con funcionalidades de otros productos. Snoop Consulting por ser una empresa de nicho, tenía mayor conocimiento que el promedio del mercado sobre distintas tecnologías. Por ejemplo, mejorar la performance de una base de datos evitaba la compra de hardware, que a su vez evita la compra de más software que debe adicionarse al comprarse más servidores. Este ahorro de costos comenzó a ser evidente a partir de la salida del 1 a 1.

Por el otro lado, se puede explicar el modelo de venta consultiva que instrumentó Snoop Consulting desde sus comienzos. No es trivial el contexto del mercado de tecnología. Hacia fines del 2000, todavía quedaban los resabios del Y2K. Las empresas habían realizados grandes gastos en tecnología. Las ventas se desarrollaban sin grandes seguimientos y las compañías de SOFTWARE estaban acostumbradas a recibir las órdenes de compra por el fax. El hecho que Snoop Consulting tomara una política de venta consultiva permitió estar más elásticos y entrenados ante el cambio de la demanda luego del derrumbe económico, donde el entendimiento de la necesidad del cliente era crucial.

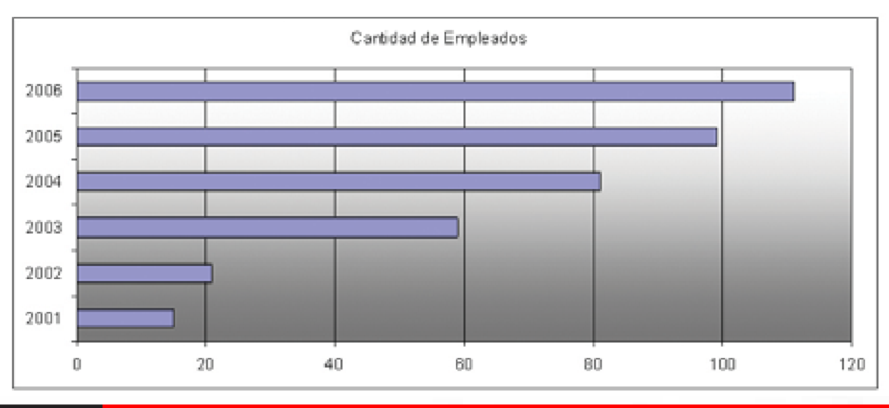
En el plano interno podemos marcar que el mayor desafío fue crecer tan vertiginosamente durante la mayor parte del tiempo, incluso en estos momentos, que incrementamos nuestra plantilla de personal en 15% en solo dos meses.

El fuerte crecimiento genera continuos embates y definiciones de procesos. Aparecen actividades no planificadas, que no se sabe a ciencia cierta si durarán en el tiempo o es solo algo momentáneo. El managment y la organización interna fueron y son actividades sobre las que estamos trabajando y poniendo foco continuamente ya que la evolución de la empresa es algo que modifica el contexto interno.

Como muestra de esta evolución presentamos dos gráficos donde se informa la evolución de la facturación y de la cantidad de personas vinculadas a Snoop Consulting (Cuadros 1 y 2).



Evolución de la facturación en miles de pesos. El dato para 2006 es pronosticado.



Cantidad de Empleados, 2006 a febrero.

Riesgos de comenzar con una compañía emprendedora

Comenzar con un emprendimiento es tomar riesgos. Los socios de Snoop Consulting teníamos trabajos en relación de dependencia y dejamos todo por llevar adelante a la compañía. De alguna manera "quemamos las naves". Esa decisión es personal e intransferible. Creo que todos tenemos una chance en la vida para iniciar con una actividad propia. Los riesgos están siempre presentes.

Una vez insertados en el mercado, la actividad nos fue formando. No obstante nos encontramos con un tema que no veíamos como problemático: trabajar con empresas grandes.

La complejidad de las empresas se incrementa con el tamaño de la misma, por lo tanto a medida que accedíamos a clientes más importantes más era la dificultad para entender los procesos y disposiciones. Por ejemplo, los tiempos para firmar un contrato, para facturar después de haber prestado el servicio, etc. etc. plantean que haya que planificar y tener en cuenta factores financieros adicionales a los propios del negocio del SOFTWARE.

Cuales fueron los factores críticos para el éxito

Los factores críticos para el éxito fueron: la misión de la empresa llevada en la médula, una política de reclutamiento y retención de recursos humanos efectiva y la manera de pensar el futuro por los socios mas allá de un periodo de tiempo. Pensar una empresa grande y consolidada, con extensión internacional cuando todavía éramos menos de una decena de personas.

Entrando en temas más tácticos u operativos, que tal vez parezcan insignificantes pero que considero uno de los factores para el éxito, es entender el costo de oportunidad. Por ejemplo, los socios que trabajan en Snoop Consulting tienen un sueldo independientemente de su participación accionaria y se lo registra contablemente de manera que el resultado del período no se encuentre "subsidiado" por una remuneración a cargos directivos camuflada en el reparto de utilidades.

Que los costos sean los correctos, que se entienda el costo de oportunidad, que los datos sean claros de forma que las decisiones puedan tomarse con la información real y fidedigna es la base para toda organización sana.

Snoop Consulting, en los años de vida no ha tenido ningún ejercicio con pérdida. No obstante el crecimiento sostenido necesita invariablemente de capital. La re inversión fue la manera en que llevamos adelante este crecimiento, sin embargo considerar capital de terceros también es un camino a seguir.

Mirando atrás, cuando comenzamos a construir los cimientos de Snoop, era todo un desafío. Dejamos nuestras actividades y nos dedicamos de lleno a llevar adelante el proyecto, otro factor clave para el éxito. Eso que todos de una u otra manera tenemos como objetivo en la vida, transformar nuestras ideas en cosas concretas. La idea de una empresa que aporte soluciones con la utilización de la tecnología de punta. Transformar el invento en innovación. Nuestra misión. ■



SERVIDORES
al alcance de todos

Servidores en PyMEs
y Corporaciones
Nota 2 de 2

Ing. Marisabel Rodriguez Bilardo
Ingeniera en Electrónica

Las aplicaciones críticas de las empresas necesitan equipos estables y con gran capacidad de procesamiento. Los grandes proveedores de tecnología están acercando a las pequeñas empresas soluciones que les permiten mejorar su infraestructura de sistemas y aumentar la productividad.

¿Qué es un servidor?

Las razones para utilizar un servidor en una empresa pueden ser muchas: se necesita centralizar el acceso a los datos, compartir recursos, backups de una red completa; y cada Administrador puede agregar más todavía. De acuerdo al perfil de la organización y la capacidad de procesamiento que se vaya a necesitar, ya existen en el mercado tendencias definidas y marcas líderes entre las cuales se puede elegir.

La implementación de un Servidor puede aumentar la productividad y eficiencia de su compañía, estimular la eficacia y rentabilidad de su negocio, hacer que sea más competitivo gracias a herramientas de productividad como el correo electrónico o el acceso a Internet, se pueden compartir recursos como las impresoras, tener un punto central de almacenamiento para sus datos y aplicaciones, en fin, dinamizar el acceso y aprovechamiento de los recursos disponibles.

En nuestro país, cada vez más, las Pymes de hoy se están profesionalizando paulatinamente, y también van teniendo más acceso a mejores tecnologías porque las grandes marcas ofrecen soluciones a su alcance. Hay muchísima variedad de ofertas y también soluciones a medida para cualquier tipo de organización.

Nos proponemos en este artículo, revisar los puntos a tener en cuenta, y además dar una idea de cuál sería el hardware más propicio para cada empresa según la implementación que necesita.

A través de los años, la definición de Servidor se fue diluyendo, de tal forma que no queda muy claro para el público en general a qué se refiere. En la jerga común solemos emplear el término "servidor" para referirnos al hardware en sí, que corre un sistema operativo y aplicaciones específicas para desempeñar tal tarea, pero originalmente un servidor consistía simplemente en cualquier máquina que corriese “servicios” a los cuales se accedía vía la red.

Con el tiempo, el término Servidor se adoptó para describir máquinas con grandes microprocesadores, con grandes capacidades de procesamiento, fuentes de alimentación redundantes, diseñadas para operar las 24 horas, todos los días, también con memoria suficiente y corrección de errores (ECC - Error Correcting Code), protección ante pérdida de datos en los discos (RAID - Redundant Array of Independent Disks), entre otras muchas cosas.

Debido a la gran demanda de computadoras con grandes capacidades de procesamiento, las marcas líderes del mercado, desarrollaron Servidores cada vez más poderosos. HP, IBM y Dell están diseñando equipos con alta densidad de procesamiento, como por ejemplo los "Blade Servers". Estos Servidores incluyen un determinado número de computadoras, por ejemplo 14, cada una dentro de un módulo de alta densidad denominado "Blade", en el espacio ocupado típicamente por una sola.

Clases de Servidores

Desde la perspectiva del software, los Servidores se pueden clasificar según el rol que cumplan en la red, por ejemplo:

- Servidores de Archivos e Impresión: Sirven para compartir dichos recursos.
- Servidores de Aplicaciones: Guardan centralizada-

mente bases de datos, software corporativo para que muchos usuarios accedan a través de la red.
- Servidores de Correo o Web
Con respecto a las categorías de Servidores según sus prestaciones, podemos empezar hablando de los de "Entry Level", los más sencillos. Cuestan alrededor de U$D 1000 y apenas pueden llamarse Servidores. En general se usan solamente para compartir archivos, impresoras o aplicaciones muy sencillas.
La mayoría tiene un solo procesador, con entre 128M y 512M de memoria, hasta 4G y discos rígidos SCSI o IDE. Los procesadores suelen ser Pentium o Athlon. También incluyen chipsets específicos que balancean el uso de la CPU, la memoria, y el manejo de I/O de datos.
En segundo lugar, se encuentran los Servidores de nivel medio, que cuestan entre U$D 1000 y U$D 10000, ocupan desde 1 a 4 unidades de rack. Tienen mucha más capacidad de procesamiento, y son capaces de trabajar en Cluster. Tienen entre 4 y 8 procesadores, 32GB de RAM y 10 o más discos SCSI. Se suelen configurar en RAID para proteger los datos. Por lo general se busca que se puedan sacar y poner discos sin tener que reiniciar el equipo, ya que la idea es tener en producción las aplicaciones que alberga la mayor parte del tiempo posible.
Otra clase de Servidores muy populares últimamente son los "Blade". Se insertan dentro de un chasis que permite compartir elementos comunes, como la ventilación, los switches de red o la alimentación, con lo cual se reduce el consumo eléctrico, los cables y los sistemas de enfriamiento.
Finalmente, los Servidores de línea alta: Enterprise o High End. Por lo general se utilizan en empresas que desarrollan negocios grandes y necesitan gran capacidad de procesamiento. El precio va desde U$D 5000 hasta U$D 45000 o hasta donde se quiera. Depende de la cantidad de discos, los procesadores, la memoria y la marca.

Qué fijarse antes de comprar

Elegir un Servidor puede ser un proceso algo tedioso pero no tiene por qué serlo. Basta con tener bien en claro lo que se necesita y planificar lo que se va a necesitar a futuro, pero sobre todo el presupuesto con el que se cuenta, no solo para comprarlo, sino para tener soporte de los proveedores ante cualquier inconveniente.

- Calidad y confiabilidad -

La confiabilidad que brinda un Servidor es de importancia clave para el funcionamiento de la red. Es importante elegir un Servidor que garantice un alto grado de disponibilidad, protegiendo y maximizando el tiempo de servicio de la red. El costo del tiempo de inactividad de la red puede ser alto y en el peor de los casos se puede llegar a la pérdida datos. (Por ejemplo, la pérdida de negocios, el descontento de los clientes o la recuperación de datos).
Por lo tanto, a la hora de elegir, el Servidor debe tener características de confiabilidad, un Servidor que pueda reconocer y avisar ante cualquier problema posible, antes de que ocurra alguna pérdida de información o de servicio. Por ejemplo: si una unidad de disco duro muestra señales de falla, ésta debería tener la capacidad de avisar de manera proactiva, a fin que se la cambie o arregle antes de que deje de funcionar y se pierda el acceso a la información sensible de la compañía.
Esto es relativo, según qué importante es la red en la empresa, en base a ello, hay que asegurarse de comprar un Servidor que incluya la confiabilidad que se necesita, como memoria ECC (memoria con comprobación y corrección de errores), controladores de matriz de unidades de disco y unidades de disco duro que se pueden cambiar sin necesidad de apagar el Servidor ("Hot Swap").

- Evaluación de la capacidad de expansión -

Un Servidor debe ser fácil de ampliar y agregar componentes. Esto protege las inversiones del la Empresa. Si se puede aumentar la capacidad de un Servidor gastando unos pocos dólares en vez de invertir en otro, se ahorra mucho dinero. Algunos Servidores han sido diseñados para ser fáciles de ampliar con sólo conectar los componentes en los slots y compartimientos libres. Esta facilidad de expansión brinda mucha flexibilidad para adaptar el sistema rápidamente a las cambiantes necesidades comerciales y tecnológicas. La mejor manera de evaluar la capacidad de expansión es asegurándose de que disponga de un mínimo de:
- 4 ó 5 ranuras de expansión PCI o PCIX adicionales
- 3 ó 4 compartimientos para unidades
- Capacidad de almacenamiento externo

- ¿Cómo evaluar la compatibilidad? -

Hay que asegurarse de comprar un Servidor que cumpla con las normas de la Industria. Esto garantiza compatibilidad con la más amplia gama de productos de hardware y software en el mercado. Entre los componentes estándar más comunes que conviene tener en cuenta se incluyen los siguientes:
- Memoria: ¿Se puede ampliar con módulos DIMM estándar?
- Unidades de disco duro adicionales: ¿Son compatibles con Wide Ultra 320 o Wide Ultra 3?
- Software de sistema operativo de red: Hay que averiguar si el Servidor fue probado y optimizado para ejecutarlo.
- Tarjetas de interfaz de red (NIC): Las redes standar son Ethernet o Token Ring; Las implementaciones estándar para utilizar una tarjeta de interfaz de red en un Servidor son PCI (interfaz de computadora personal).

- Escalabilidad -

Escalabilidad significa la posibilidad de aumentar el rendimiento y la funcionalidad, una consideración que se vuelve muy importante a medida que aumenta el número de usuarios o si se utilizan aplicaciones que implican una mayor carga sobre la red. Es mejor elegir un Servidor nuevo que pueda adaptarse a sus necesidades, que comprar un Servidor nuevo cada vez que las necesidades cambien:
- ¿Se podrá agregar características adicionales más adelante para aumentar el rendimiento? (por ejemplo: Memoria adicional, un controlador de

HP Compaq Proliant ML350 G4



Procesador Intel® Xeon 3.2 GHz Caché: 1 MB con tecnología EMT64 Extended Memory 64 Technology9 e Hyper Threading
Memoria base: *1024MB de memoria PC2700 DDR SDRAM a 333MHz*
Memoria máxima: *8 GB*
Controladora: *Integrada de doble canal Ultra320 SCSI ó bien controladora Smart Array 641 pre-instalada en modelos array.*
Disco: *36,4 GB a 15Krpm pre-instalado sólo en modelos SCSI non-hot plug. Sin disco pre-instalado modelos SCSI hot-plug.*
- Slots de expansión
- 1 x PCI-X 64bits/133MHz
- 2 x PCI-X 64bits/100MHz
- 1 x PCI-X 64bits/66 MHz
- 1 slot PCI-Express 4x
- 1 slot PCI-Express 8x
Tarjeta de Red: *Tarjeta de red integrada NC7761 PCI Gigabit*
Gráficos: *Controladora de video ATI RAGE XL integrada, con 8MB SDRAM de memoria de video.*

matriz de unidades de disco)
- ¿Es posible actualizar fácilmente a un procesador más rápido o a múltiples procesadores si su empresa lo necesita más adelante?
- ¿Qué incremento en la potencia de procesamiento proporciona un procesador adicional? La respuesta a esta pregunta depende mucho del diseño del sistema y varía enormemente según el Servidor. Por eso, debe insistir en que le proporcionen información sobre el rendimiento.

Los controladores RAID son dispositivos especializados que pueden añadir un impresionante grado de rendimiento y confiabilidad a su subsistema de unidades de disco duro. Los controladores RAID a menudo controlan varias unidades de disco duro a la vez, protegiendo sus datos y facilitando el acceso más rápidamente de lo que sería posible de otro modo. Existen varias implementaciones RAID, dependiendo qué tipo de redundancia se desee, el fabricante debe proveer herramientas suficientes para crear los RAIDs y monitorear su funcionamiento.

La utilización de sistemas de almacenamiento tolerantes al fallo es imprescindible actualmente en la configuración de un Servidor de datos. Diferentes estudios demuestran que el costo de la pérdida de datos, sumado al costo del tiempo durante el cual el sistema no está en explotación, es superior al costo de un sistema RAID.

RAID es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante. Ofrece mayor tolerancia a fallos y más altos niveles de rendimiento que un sólo disco duro o un grupo de discos duros independientes.

RAID ofrece varias opciones, llamadas niveles RAID, cada una de las cuales proporciona un equilibrio distinto entre tolerancia a fallos, rendimiento y coste.

Oficialmente existen siete niveles diferentes de RAID (0-6), definidos y aprobados por el el RAID Advisory Board (RAB). Luego existen las posibles combinaciones de estos niveles. Los niveles RAID 0, 1, 0+1 y 5 son los más populares.

Los Servidores de HP línea DL incluyen la controladora de arreglos de como estándar. De esta forma, la controladora está incluida en el precio del Servidor sin agregar un costo adicional.

Dell ofrece un software llamado Array Manager, que permite armar los arreglos de discos, intercambiarlos y monitorearlos. El log de eventos es muy completo. Ante alguna falla, hace falta solamente marcar como "Off Line" el disco fallado, reemplazarlo y luego automáticamente el software avisa que ha iniciado un "Rebuild" (reconstrucción) del arreglo de discos, para recuperar la redundancia. Este proceso demora al menos una hora. Esta aplicación forma parte del software adicional que viene con los servidores Dell, que es una biblioteca con todos los drivers, softwares de monitoreo y diagnóstico, booteo y documentación, que son fundamentales para los Administradores. "Dell Open Manage" permite conectarse via web al Servidor y saber el estado de todo el hardware.

Servidor Sun Fire T 2000

Triple rendimiento, la mitad del consumo y la mitad del tamaño. Nunca se había ofrecido tanto rendimiento en un servidor tan compacto, y mucho menos en uno que puede ahorrarle millones en costes de alimentación y refrigeración. El servidor Sun Fire T2000 es un descubrimiento sin precedentes que redefinirá el futuro.

Procesador UltraSPARC T1 de 8 núcleos a 1,2 GHz Arquitectura con SPARC V9, protección de ECC, Caché por procesador,16 KB de instrucciones,8 KB de caché de datos principales y 3 MB de L2 integrada

Con el incremento de los precios de los recursos energéticos, y cada vez más computadoras conectándose a las redes, Sun se comprometió a que sus equipos consuman lo menos posible minimizando el derroche de energía, garantizando un redimiento superior.

- Controladores y unidades de disco duro -

Las unidades de disco duro y otros dispositivos de entrada/salida por lo general interactúan con el Servidor por medio de un controlador SCSI. Wide Ultra320 es un estándar relativamente nuevo que contribuye a garantizar un funcionamiento rápido con el subsistema de almacenamiento del Servidor, a la vez que brinda espacio para disponer de ancho de banda para entrada/salida en el futuro.

Sea cuál sea el estándar que elija, las unidades de disco duro en su Servidor deben contar con el apoyo del controlador.

Los Servidores HP incluyen controladores Wide Ultra3. No todas las compañías integran estos controladores. Al momento de evaluar un Servidor, hay que averiguar si habrá costos adicionales para un controlador y si el controlador ocupa una valiosa ranura de expansión.

Características a tener en cuenta

Microprocesador: Se usan por lo general de 1 a 4, de 32bits de AMD o Intel Xeon, con Sistemas Operativos Linux o Windows. También se utilizan procesadores de 64 bits con UNIX. Otro tipo de procesador es el G5 de Macintosh.

Memoria: El tipo más común es la llamada ECC, que contiene circuitos específicos para detectar y corregir errores sin detener el sistema. Los Servidores de "Entry Level", los más pequeños, por lo general soportan 4G, y los mayores utilizan de 1GB hasta 32GB.

Con respecto a la conectividad, las placas de red suelen ser entre 1 y 4 y tener una velocidad de 1GB. Si los Servidores deben formar parte de una red de alta velocidad, o una SAN ("Storage Area Network"), hay que agregar las interfaces adecuadas para conectarse a los dispositivos que correspondan, por ejemplo, interfaces de Fibra para comunicarse con switches de Fibre Channel.

El sistema más utilizado para Servidores en lo que respecta a discos rígidos es SCSI o sino ATA, que tienen altas velocidades de rotación. Los de menor capacidad usan más bien IDE. Tener varios discos permite armar configuraciones RAID para proteger los datos y tener redundancia. Un tamaño adecuado es de entre 36 y 146 GB.

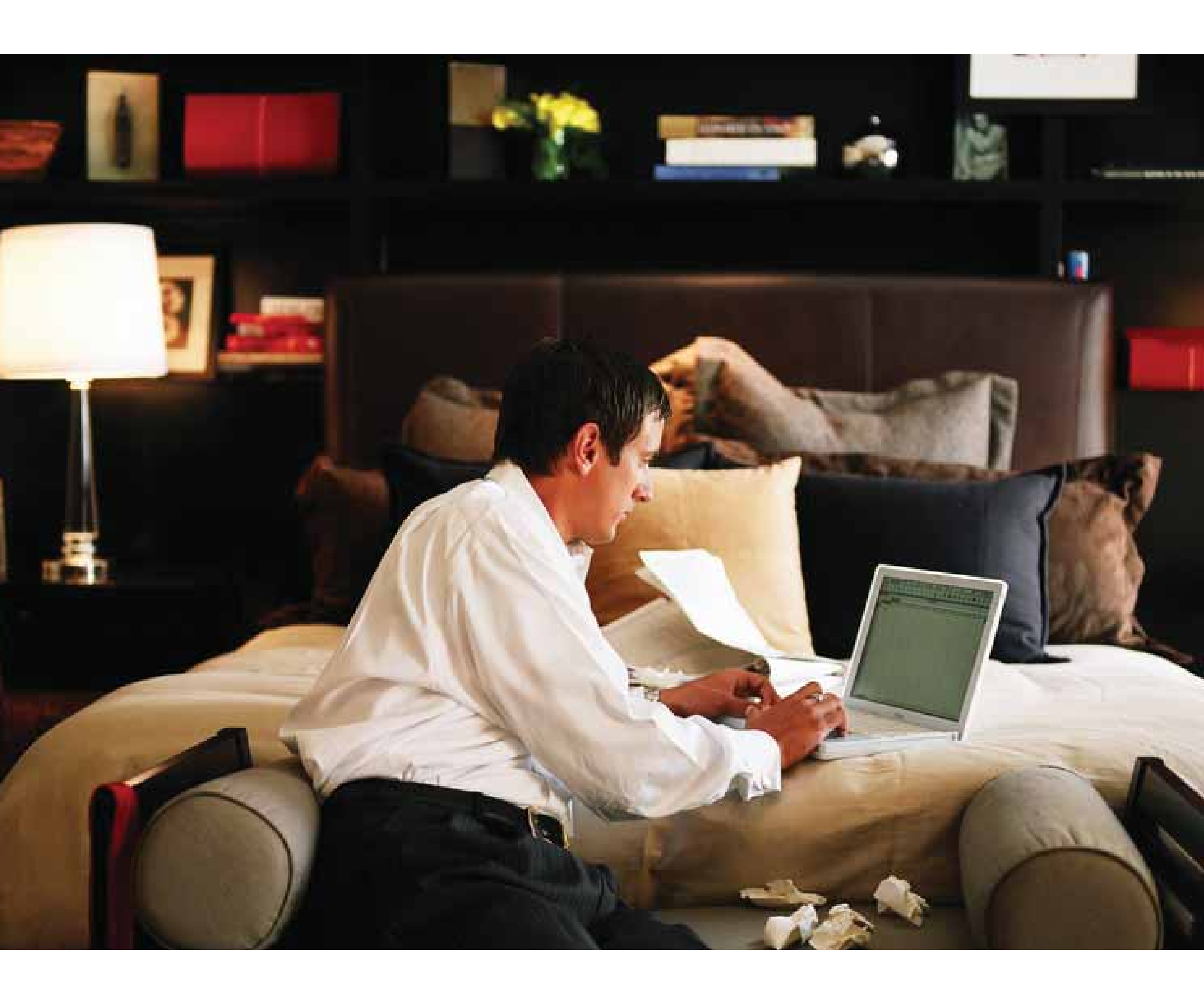
Las grandes marcas

Los fabricantes más importantes de Servidores son Dell, HP, IBM y Sun. Sun se dedica mayormente al mercado de UNIX para clientes grandes, aunque sus Servidores soportan muchas plataformas. Otros fabricantes son Hitachi, Gateway, NEC, SGI y Acer. Hay marcas nacionales como ARM y Axus que fabrican Servidores con procesadores Intel.

Dell, desde su nacimiento, utiliza un modelo de ventas llamado "Build to order", y es un caso de éxito estudiado por las Universidades. Consiste en que el mismo cliente diseña primero el equipo según lo que necesite, y luego se fabrica. Lo que se ahorra en no mantener un stock fijo y la flexibilidad que se tiene a la hora de instalar un Servidor nuevo según los requerimientos específicos, es una de las claves del éxito de esta empresa. Los modelos se llaman Power Edge. Para la filial argentina, los pedidos se envían a Porto Alegre, en Brasil. Los modelos y las configuraciones pueden consultarse en la página de Dell.

Los Servidores de IBM que se están comercializando actualmente están dentro de la línea Xseries, que utilizan procesadores Intel. Hay para niveles "entry", que pueden valer entre U$D 750 y U$D 2000 (modelos XSeries 226,336 y 346), luego la línea media, cuesta hasta U$D 5000, aunque el añadido de discos, cables, entre otras cosas, puede duplicar el valor del Servidor. En la página de IBM se pueden encontrar las características y los precios de todos los equipos disponibles.

HP ofrece Servidores con procesadores Xeon. Las líneas de Servidores para Pymes se llaman Proliant y los Blade System. Los modelos pueden verse en la página de HP, los precios comienzan desde alrededor de $1000.



e-learning

Fredi David Vivas

Líder de Estrategias de Comunicación de Microsoft IT PRO Argentina
www.itpros-argentina.com.ar

Cuando se diseña una experiencia educativa, es claro que las más exitosas son aquellas que se basan en crear una comunidad. Reunida la comunidad, ésta se enfrentará a diversos contenidos preestablecidos o espontáneos que al final generarán conocimientos en cada uno de los participantes.

Reforzando el sentido de colaboración y comunidad

En gran medida, la clave de la educación virtual está en que se basa en ese principio. Primero hay que reunirse para luego aprender. Y reunirse significa conocerse, participar, aportar y aprender de los demás. Los cursos que funcionan bien centran su esfuerzo en establecer un clima de confianza y colaboración para a partir de allí, empezar a recorrer los temas que se proponen aprender.

Algunas de las estrategias para crear un ambiente interactivo en un curso virtual incluyen: estudios de casos, narración de experiencias, demostraciones, juegos de roles, simulaciones sociales, grupos de discusión, carteleras de avisos, talleres asistidos y tutorías personalizadas.

Se pueden crear ambientes más estimulantes promoviendo el razonamiento crítico en grupos de trabajo virtuales reducidos, más que en un gran salón de clase superpoblado conducido por un profesor.

¿Cómo es un curso virtual?

La pieza básica de la educación virtual, al igual que en la educación presencial, es el aula (también virtual). Nada más y nada menos que un punto de reunión. Privada, temporal, con un objetivo específico. El profesor y los estudiantes deciden lo que quieren hacer dentro de ella. Cada curso es un evento único y así como pueden existir elementos y materiales predeterminados, el desarrollo del curso es impredecible. Cada aula es un mundo aparte capaz de reflejar el estilo propio de cada profesor y la dinámica del grupo de alumnos en un período de tiempo determinado.

El profesor cuenta con herramientas de trabajo simples pero poderosas y con ellas sus alumnos pueden:

- Examinar un elemento de contenido dentro del curso (archivos de texto, imágenes, videos o audios)
- Visitar una dirección en la Web (un enlace externo al curso)
- Participar con su opinión en un foro de discusión y examinar los aportes de los demás alumnos
- Contestar una serie de preguntas sobre el tema y comprobar su comprensión.

Toda la información que el profesor agregue al curso se mantiene en su aula virtual. Es equivalente a pensar en un salón de clase en el que la noche anterior el profesor escribe en la pizarra su lección, deja en cada asiento un documento para que lo analicen los alumnos, inicia un tema de discusión en la cartelera y prepara un cuestionario para que lo contesten.

Profesores y alumnos cuentan con buzones de correo electrónico personales para el intercambio de mensajes permanentemente. Cada vez que el profesor regresa a su aula encuentra las actividades desarrolladas por los alumnos y prepara el trabajo de la siguiente sesión.

Algunas ventajas de la educación virtual

Dentro de las razones que se mencionan para considerar la educación virtual, como una alternativa seria y presente, están la reducción de costos, el acceso de nuevos públicos a la tecnología y el mayor compromiso de todos los participantes en el proceso educativo. Varios elementos se destacan en este nuevo esquema de aprendizaje:

Experiencia - El estudiante virtual se ve involucrado en una nueva experiencia social y de aprendizaje que puede incluir comunicaciones directas con su profesor, discusiones con sus compañeros de curso o estudio individual de contenidos a su propio ritmo.

Compromiso - Los cursos virtuales ofrecen una oportunidad única al estudiante de compartir experiencias con otros, lo que refuerza el sentido de colaboración y de comunidad. Además el estudiante recibe el control de su tiempo y sus recursos. Ésto le permite elegir el mejor camino de aprendizaje de acuerdo con sus preferencias y capacidades.

Flexibilidad - Desde cualquier lugar y a cualquier hora, los estudiantes pueden tener acceso a sus cursos virtuales. Se estima que aproximadamente el 80% de las empresas ya tienen solucionado su acceso a Internet, por lo que los obstáculos técnicos de acceso de los estudiantes que trabajan ya están prácticamente superados.

Actualidad - Los profesores tienen la oportunidad de actualizar sus materiales y temas de discusión instantáneamente; ésto logra cursos frescos y consistentes con la actualidad.

Personalización - Aunque parezca contradictorio, la educación virtual permite un fluido contacto personal entre el profesor y el alumno. El intercambio de mensajes escritos y la posibilidad de seguimiento detallado del progreso, le dan al profesor un conocimiento del alumno muchas veces mayor que en cursos presenciales.

¿En qué beneficia a las instituciones?

Una de las grandes ganancias al pasar los cursos (o parte de ellos) al mundo digital es que la institución comienza a tener un registro tangible de su patrimonio académico. La base de su talento educativo ya no está solamente en las mentes de sus maestros, sino que se transfieren a un sistema de administración de contenidos efectivo y perdurable.

Otros factores interesantes:

Uniformidad del contenido - La información básica que se presenta en los cursos es consistente para todos los estudiantes reduciendo la posibilidad de errores de interpretación. También es consistente entre grupos diferentes del mismo curso.

Totalmente a medida - La información puede adaptarse a los diferentes usuarios debido a la modularidad de los contenidos. Los cursos y programas pueden ser modificados teniendo en cuenta el público al que van dirigidos. Un mismo curso puede ser adaptado, según las necesidades relevadas de cada área a capacitar.

Modularidad de la presentación - Los cursos se pueden construir con una arquitectura de módulos intercambiables, lo que facilita el desarrollo de nuevos eventos de aprendizaje de diferente tamaño y duración. Redistribuyendo esos módulos, se puede construir un curso con un contenido diferente en muy corto plazo.

Administración y seguimiento - Los sistemas de capacitación virtual permiten la medición y el seguimiento de la efectividad de un curso. Toda la actividad de los alumnos y su interacción con los profesores es registrada, de manera que se pueden detectar y corregir las debilidades rápidamente. Además de evaluar el desarrollo de los estudiantes y la eficacia del aprendizaje.

Control y manejo de la información - A medida que nuevos productos educativos son desarrollados y las versiones viejas se vuelven obsoletas, se crea el reto para los administradores de los contenidos de mantener su biblioteca de cursos actualizada y completa. La institución se ve obligada a crear un sistema organizado y efectivo de archivo digital.

Aporte colaborativo - El archivo de documentos y módulos educativos se enriquece constantemente con los aportes no solo de los profesores sino también de los estudiantes. Cada nuevo curso es más completo y actual. Un glosario de términos de una disciplina, por ejemplo, se va construyendo con nuevos vocablos en cada edición del curso a partir de los aportes de los participantes.

¿Qué es el Blended Learning?

Lingüísticamente hablando, si buscamos en un diccionario podemos encontrar la definición del término blend: mezclar, combinar. Así que, blended seria mezclado, combinado... y por lo tanto, no estaríamos equivocados en hablar de modelo mixto.

Pedagógicamente hablando, podríamos decir que se trata de diseñar un curso combinando sesiones presenciales y fases a distancia. De esta manera, el Blended Learning no es una invención asociada la era del E-Learning, sino que tiene tanta antigüedad como la educación a distancia; que lleva practicándose desde principios del siglo XX.

Esto es, principalmente, porque cuando hablamos de E-Learning siempre veo implícita la faceta Blended; es decir, no pienso en cursos 100% a distancia, sino que me gusta considerar el E-learning como un sistema flexible de formación a distancia, apoyado en las TIC (tecnologías, redes de telecomunicaciones, videoconferencia, TV digital, materiales didácticos multimedia...) que permiten según las circunstancias y las características de cada acción formativa, combinar diferentes elementos pedagógicos: la instrucción clásica (presencial o de autoformación), la realización de actividades, los contactos en tiempo real (presenciales, videoconferencias, chats...) y los contactos diferidos (consultas al tutor, foros de discusión, correo electrónico, etc.)

¿Cómo elegir el modelo de enseñanza - aprendizaje que se ajuste a mi necesidad?

Es importante no caer en la tentación de recomendar el Blended Learning como la mejor solución para todos los casos; ni tampoco el E-Learning 100% a distancia.

Cada situación tiene su solución óptima. Antes de proceder al diseño de un curso (ya sea presencial o de E-Learning), deberíamos analizar el contexto del mismo: necesidades formativas, características de los usuarios finales, recursos disponibles (humanos, económicos, materiales... etc.). A partir de la información obtenida, podremos decidir si es conveniente que el curso se desarrolle de forma presencial, 100% a distancia o bajo una visión Blended Learning. Por tanto, el hecho de combinar sesiones presenciales con fases formativas a distancia (Blended Learning) no nos asegura, de por si, una formación de calidad.

La motivación: un factor indispensable

Seria bueno realizar, como mínimo, una sesión presencial de presentación del curso y una sesión presencial de clausura del mismo como elemento motivador, sobre todo cuando se trata de acciones formativas dirigidas a usuarios no habituados a la formación a distancia ni al E-Learning.

Además, puede ser recomendable alternar sesiones presenciales con fases de aprendizaje a distancia, en función de la duración del curso y las características del mismo. Estas sesiones presenciales pueden tener varias finalidades:

- Motivar (con el simple hecho de asistir a la sesión) al alumnado que no está habituado a la formación a distancia,
- Resolver dudas de los estudiantes,
- (Auto) evaluación y seguimiento del trabajo realizado hasta el momento,
- Presentar los siguientes contenidos a trabajar en el curso y muy importante,
- Realizar actividades que no puedan ser realizadas a distancia (sobre todo algunas relacionadas con el desarrollo y aprendizaje de habilidades).
- Por otro lado, si el diseño instruccional y los recursos metodológicos empleados en el desarrollo del curso son adecuados, los resultados de una acción formativa completamente a distancia pueden ser perfectamente satisfactorios.

El éxito de una acción formativa (ya sea mixta o a distancia) reside, en gran parte, en la labor tutorial y en la vivencia del grupo-clase (ya sea grupo presencial o grupo on-line). Un alumno puede llegar a desmotivarse completamente si se siente solo: bien porque el profesor de la asignatura (o curso) no dinamiza adecuadamente el aula y/o no promueve un clima grupal adecuado, o bien porque el curso está enfocado de forma que no se contempla la interacción entre alumnos (alternativa, esta última, perfectamente válida, pero que conlleva un mayor riesgo de desmotivación en los alumnos).

Conozcamos más de este tema junto a expertos de Edgardo Visñuk & Asociados, consultora especializada en desarrollos E-Learning.

-¿Qué aspectos se tienen en cuenta a la hora de iniciar un desarrollo E-Learning? y ¿Cuáles son los principales tips a relevar para conocer a fondo las necesidades del cliente?

En la primera etapa de consultoría realizamos un diagnóstico en una o varias entrevistas con los referentes temáticos de la empresa-cliente. Relevamos las necesidades del cliente de acuerdo con cinco puntos:

- Los objetivos de la capacitación: qué deben aprender los destinatarios y qué tareas o habilidades se espera que los mismos puedan realizar luego de la implementación.
- Los destinatarios: cuántos son, qué cargos ocupan, dónde se ubican, responsabilidades, etc
- El contenido a implementar: ¿Son tareas, son habilidades?
- Los recursos económicos o inversión que está dispuesta a realizar la empresa.
- Las posibilidades tecnológicas con las que cuenta tanto la empresa como cada uno de sus recursos humanos.
- La duración de la implementación: esto determina el tipo de desarrollo a realizar.



-¿Cuál es la tendencia en relación a plataformas, estándares y lenguajes para la creación de proyectos E-Learning?

Los diseños se realizan de acuerdo con los estándares de la industria: SCORM Versión 1.2 LMS RTE3 SCORM 2004 CAM and RTE, IMS, AICC Java Scrip &AICC HACP AGR-010, VCalendar.

-Tomando como referencia el rápido crecimiento de los cursos a distancia ¿Qué proyección tiene en los próximos años y cuales son las principales barreras a derribar?

Las capacitaciones de tipo E-Learning se están orientando fuertemente hacia los simuladores dentro del mismo ámbito laboral. Los simuladores son una herramienta para que el participante realice efectivamente las tareas que se le pide incorpore luego de la capacitación. Este tipo de desarrollos tiene muchas ventajas y una desventaja: son costosas porque son difíciles de desarrollar. Pero los beneficios son muy altos: entre otras ventajas, permiten una transferencia a la tarea casi inmediata ya que el participante puede practicar verdaderamente las tareas que se le demandarán y además, ¡puede equivocarse!.

Los juegos en capacitación no son una novedad, pero sí es algo que se está imponiendo como tendencia en el mercado. Son divertidos y por lo tanto producen un nivel positivo de participación y también de interacción social. Claro que muchas empresas no apuestan a este tipo de desarrollos porque tienen la visión de que una capacitación debe ser seria o que el empleado que juega está perdiendo el tiempo.

Otra de las tendencias es el M-Learning: "Aprendizaje Móvil" o capacitación a través de celulares u otras tecnologías móviles. Aquí se utilizan mucho los recursos multimedia o las conexiones son on-line, lo que permite al participante tener acceso permanente e instantáneo a los contenidos de aprendizaje. Éste es un recurso de alto impacto para destinatarios que se desempeñan mayormente fuera de la empresa, visitando a clientes o en tareas de tipo operativas. El M-Learning permite, por ejemplo, chequear el perfil del cliente o la secuencia de operaciones a realizar antes de la cita o tarea a realizar.

Las barreras a derribar son en principio económicas: aunque más tarde se economice en tiempo, salas, etc, se requiere una inversión inicial en el desarrollo de éstas herramientas. Además, es preciso contar con instructores capacitados en éstas tecnologías y que además dispongan del tiempo suficiente para dar feedback. Pensemos, respecto de esto último, que la cantidad de participantes suele ser más numerosa y la falta del contacto "cara a cara" hace que sea mayor la demanda hacia los capacitadores. En segundo lugar podemos mencionar la barrera tecnológica: todos los participantes deben tener acceso a computadoras, celulares, etc y además tiene que existir soporte técnico debidamente capacitado y disponible durante todo el proceso. Finalmente, se necesita contar con una dosis de confianza desde la empresa solicitante respecto de sus empleados ya que, de no existir un seguimiento de las actividades o mediciones permanentes, aquéllas se sostienen desde la honestidad académica de los participantes, esto es, de la responsabilidad de los mismos frente a su propio auto-aprendizaje.

Go!

PuntoSCORM: Foro de estándares eLearning
http://www.elearningworkshops.com/

Seminarios abiertos y experiencias para vivir el aprendizaje
http://www.edgardovisnuk.com/

Sistema de Autenticación y Administración de Información Personal

HARDkeyMIO



HardkeyMIO es una suite de utilitarios de software asociados a una llave electrónica USB que sirve como elemento físico de autenticación y almacenamiento de passwords.
La misma está compuesta por tres módulos que permiten resolver los principales requerimientos de seguridad.



Disco Privado Virtual

Accede mediante la llave a un área virtual de la PC donde puede almacenar información en forma cifrada.





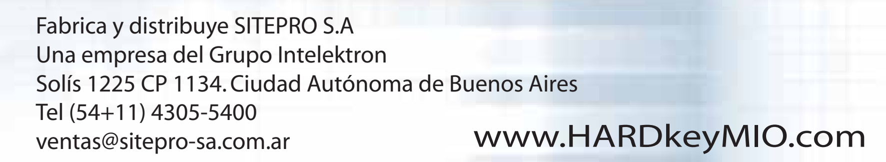
Windows Logon

Reemplaza el ingreso tradicional al sistema operativo mediante usuario y password por una llave electrónica.



Administrador de Passwords

Permite la autentificación automática en web-banking, web e-mail, etc.



Fabrica y distribuye SITEPRO S.A
Una empresa del Grupo Intelektron
Solís 1225 CP 1134. Ciudad Autónoma de Buenos Aires
Tel (54+11) 4305-5400
ventas@sitepro-sa.com.ar

www.HARDkeyMIO.com

SITEPRO
Sistemas y tecnologías de protección informática



SEGURIDAD en LINUX

Por Luis H. Otegui

De 0 a 100 en 5 notas

Nota 3

Comenzamos esta tercera entrega. Es momento de dar el salto, y pasar a ver la situación de un modo global: la realidad es que las amenazas vienen de "de afuera", y nosotros queremos defendernos de ellas. Ahora bien, ¿Qué significa "afuera"? Hoy en día, los límites, tanto físicos como lógicos, de las redes se han difuminado. Es necesario entonces ocuparnos por diagramar un esquema de trabajo, y comenzar a pensar en un planteo integral de seguridad, más que en asegurar cada host por separado.

En esta nota, nos centraremos entonces en "dibujar" un perímetro de nuestra red, comprender cabalmente de qué estamos hablando con ello, y aprender a reducirlo - para que sea más fácil de mantener- y además, para minimizar nuestra área expuesta al exterior. Trataremos además los casos referentes a la conectividad segura con redes remotas. Asimismo, revisaremos la aplicación de modelos de segmentación, para realizar una contención de daños eficaz en caso de que ocurra una intrusión, y veremos por último la aplicación de sistemas de detección de intrusiones.



Planteos en red

Redes: Bordes y Superficies

En la introducción hablé de "minimizar las superficie expuesta". Ahora bien, para realizar esta acción, es necesario conocer esta superficie. Antes, calcular o conocer la superficie expuesta de una red era una tarea más fácil. Pero en la actualidad, con los medios de acceso existentes (*WiFi, WAP, Bluetooth)* los límites se han desdibujado. Una cosa debemos tener en claro: la superficie expuesta de nuestra red no está conformada sólo por sus firewalls de borde, sino que además engloba a todos aquellos hosts que exporten alguna clase de servicio o información hacia el exterior. Ésto es así porque, como ya mencioné en una nota anterior, nuestro planteo de seguridad debe descansar sobre tres bases:

- Dejar fluir sólo la información necesaria para que todo funcione (es decir, configurar apropiadamente los firewalls, los de los hosts y los de borde).
- Monitorear la actividad de la red de manera sistemática.
- Utilizar aplicaciones lo suficientemente fuertes como para resistir ataques.

¿De qué nos valdría mantener un esquema de firewalls estricto, si nuestra seguridad puede ser vulnerada por un simple ataque de *buffer overflow* sobre alguna aplicación que corre en un servidor? Debemos aprender entonces a individualizar correctamente aquellos hosts que pueden resultar problemáticos, o cuya seguridad puede resultar comprometida. Así pues, elaboremos un mapa de la red, que nos ayude a definir la frontera expuesta de la misma.

Cartografía del ciberespacio

Si estamos planteando una red desde cero, realizar esta acción puede resultar hasta natural. Pero si debemos relevar una red ya existente, puede resultar una tarea ardua, y muy susceptible de realizar omisiones.

Comencemos entonces por catalogar como obvios componentes de la frontera expuesta de la red a algunos hosts y/o dispositivos:

- *Firewalls.*
- *Proxys.*
- *Webservers.*
- *Mailservers.*
- *Servidores FTP.*
- *Servidores de base de datos.*
- *Servidores SSH.*
- *Access points inalámbricos.*

Ahora bien, los anteriormente mencionados son los miembros más fácilmente identificables de nuestra frontera. Pero ¿Qué podemos decir de aquellos otros menos visibles, ya sea por su emplazamiento físico como por su poca utilización? Ejemplo de estos últimos lo constituyen aquellos hosts que se conectan a nuestros servidores por acceso remoto en alguna de sus varias formas, o aquellas estaciones de trabajo que envían o reciben datos desde el exterior (un servidor FTP al que suben datos algunos miembros de la empresa, y que se habilita esporádicamente, por ejemplo). Puede sonar un poco paranóico, pero cada vez que se intercambian datos con el exterior, el perímetro de la red se desdibuja, y se vuelve borroso. Y aquí es donde el riesgo aparece…

Es así que nos conviene identificar a aquellos sistemas que intercambian datos con otros externos, y pensar soluciones para asegurar estas comunicaciones.

Controlar el tráfico de las estaciones de trabajo puede resultar más o menos difícil. Si hablamos de una empresa con políticas de utilización de la red más o menos serias, estaríamos ante una tarea que no nos traería muchos dolores de cabeza. Pero si hablamos de una red del ámbito educativo -por ejemplo- la complejidad del ordenamiento puede ir de difícil a imposible. Ante todo, para tener una idea del volumen de tráfico intercambiado y detectar posibles fuentes de riesgo, es una buena idea instalar alguna aplicación de monitorización, como Ntop (www.ntop.org). Pero esperemos hasta la próxima sección para determinar qué acciones es conveniente tomar…

Políticas de ajuste

Una vez que tenemos una idea más o menos acabada del estado de nuestra red, de la dimensión de su frontera y del tráfico que la atraviesa, podemos empezar a pensar en medidas para contener posibles intrusiones. La idea rectora, como siempre, es no proporcionar a nada ni nadie más privilegios que aquellos que necesita para realizar su trabajo. Esta idea se desarrolla de diferente manera al hablar de los distintos componentes de la frontera, o de las estaciones de trabajo del interior. Con las estaciones de trabajo, hay que lidiar con el deseo de los usuarios de utilizar herramientas de mensajería instantánea, enviar correo vía algún webmail

gratuito externo, descargar contenidos vía p2p, y otras yerbas. Entre los miembros de la frontera, la aplicación de un "régimen de adelgazamiento" para hacerlos menos visibles se hace imprescindible.

Asimismo, podemos pensar -si ya no lo hemos hecho- en modificar la forma física de la frontera, diseñando y construyendo una DMZ. A ella irán a parar todos aquellos hosts dedicados a exportar servicios, y habrá que reconfigurar sus firewalls para permitir sólo aquellas conexiones entre ellos y el exterior -o interior de nuestra intranet- que sean estrictamente necesarias para que dichos servicios sean prestados. Por ejemplo: dados el ó los bastiones de la DMZ, los mismos no deberían aceptar tráfico originado en la misma y destinado a ellos (es decir, deberían existir reglas en la cadena INPUT de la tabla *filter* de IPTables que prevengan estas conexiones).

OK, ya aislamos a los hosts potencialmente más peligrosos de la frontera en un espacio controlado, y con guardias en la puertas. Ahora, debemos elegir las características más fuertes para sus pobladores, y "vacunarlos" contra las posibles infecciones conocidas hasta este momento. Es decir, debemos seleccionar el software -distribución, versiones de programas, etc.- que utilizaremos para cada servidor, y luego dedicarnos a emparchar las distintas vulnerabilidades que se hayan detectado sobre los mismos. Más tarde pasaremos a fortalecer las aplicaciones y/o lenguajes que dependen de los programas servidores. Para poner un ejemplo de lo más trivial, de nada nos valdrá tener un Apache o un Mysql en su última versión estable y con todos los parches de seguridad pertinentes, si la versión de PHP o Perl que utilizamos tiene fugas de memoria que pueden conducir a una intrusión, o a un eventual DOS por caída del servidor… o si la consulta a la base de datos está mal construida, y puede llevar a un ataque de *SQL Injection*…

El siguiente ítem a considerar (aunque no necesariamente en orden cronológico) es el cifrado de -en lo posible- todas las comunicaciones relevantes, en todos los sentidos posibles: entre el exterior y la DMZ, entre la intranet y la DMZ, y por último, entre los servidores de la DMZ mismos. Esto implica que el correo se consulte con cifrado TLS o SSL, que el webmail "viva" en una conexión con soporte SSL, y que las consultas a base de datos se realicen en lo posible vía *sockets* UNIX, o con conexiones cifradas si deben ser interservidor.

Por último, deberíamos instalar un sistema de detección de intrusiones basado en host (o HIDS) como Tripwire o AIDE (por nombrar los más simples) en cada host de la DMZ, y correrlos de manera habitual mediante una tarea de cron (conviene acordarse de actualizar la base de datos del HIDS ante cualquier actualización que realicemos, para evitar falsas alarmas).

Una vez que hemos "acorralado" aquellos hosts más problemáticos dentro de la DMZ, hemos de centrarnos en controlar el tráfico intercambiado por la intranet no dedicada a producción -estaciones de trabajo, servidores SAMBA, DHCP y DNS internos, etc.- y el exterior, y entre ella y la DMZ. Centrándonos en esto último, no deberíamos permitir las conexiones para mantenimiento de los servidores (subir páginas web, modificar bases de datos, servidores DNS o FTP, actualizaciones de software) más que desde ciertos hosts cuidadosamente seleccionados de la intranet -la razón de esto es contener una posible intrusión desde la DMZ a la intranet.

Las conexiones a direcciones Web externas deberían pasar por un Proxy de tipo Squid, con capacidades de filtrado de *malware*, y si es posible, deberíamos implementar Proxys a nivel de aplicación para FTP, SMTP y POP. Desde ya, las políticas de filtrado de conexiones del firewall deberían permitir sólo aquello que es estrictamente necesario para el desempeño normal de las tareas, pero nada más que eso. Si es posible, y para evitar *spoofing* de IP, o para minimizar el riesgo de robo de datos, se debería permitir el tráfico a través del firewall sólo en función de direcciones MAC, y no por IP. Si bien las direcciones MAC son igualmente falsificables, un buen NIDS nos puede advertir de la existencia de una MAC duplicada con más facilidad que si tratásemos con una IP duplicada. Otro caso es el de que un *hacker* que ha logrado penetrar nuestra red "fabrique" una IP para recolectar datos del tráfico interno. Si este es el caso, deberíamos detectar tráfico de dos direcciones IP referidas a una misma MAC.

Divide y triunfarás

Si debemos vérnoslas con una red grande, como ocurre en empresas de mediano o gran porte, o en ambientes educativos o gubernamentales, es inevitable pensar en realizar segmentación IP. La mayoría de las veces se piensa en crear subredes para ordenar el tráfico y disminuir los dominios de colisión y broadcast, pero además, si nos tomamos un pequeño trabajo extra, podemos prevenir que una pequeña intrusión, o un incidente de infección con virus, por ejemplo, se convierta en una catástrofe de toda nuestra red.

Es una buena idea colocar un Proxy en cada sub-unidad organizativa de nuestra intranet, o dividir la misma en función de los distintos niveles administrativos. La conectividad entra todas estas unidades o subredes puede darse a través de servidores SAMBA o de algún servidor de archivos equivalente.

Ahora bien, manejar el esquema de autenticaciones de un monstruo de varios cuerpos y varias cabezas puede convertirse en un verdadero martirio. Si debemos crear usuarios para cada subred, emplazar autenticadores en las mismas, etc., lo más conveniente puede ser, de acuerdo siempre a la escala de la red, decantarnos por una solución integradora del tipo NIS o LDAP. Ambas permiten organizar jerárquicamente el manejo de usuarios -más LDAP que NIS, porque por defecto nos invita a armar un "mapa" o esquema de la red que refleje la arquitectura real de la misma. De esta manera, cuando miremos los esquemas de autenticación, nos resultará más intuitivo relacionarlos con los usuarios reales que se sientan frente a cada estación de trabajo.

Ambos esquemas de autenticación soportan la creación de servidores delegados o esclavos, que sólo mantienen una copia de la porción relevante para su funcionamiento de la base de datos total de usuarios/grupos. Ésto es una ventaja, ya que no necesitamos autenticar a todos los usuarios de las distintas subredes en un servidor central, ni tampoco exportar toda la base de datos de usuarios a cada Proxy. De esta forma, logramos que cada subred "vea" sólo lo que necesita ver para funcionar, y además, hacemos que ante una eventual caída del servidor central de autenticación, las distintas subredes puedan seguir trabajando de forma autónoma.

Integrar NIS o LDAP con SAMBA u otra solución de autenticación y manejo de usuarios para clientes Microsoft no es una tarea trivial, pero es realizable. Esta solución tiene un nivel de confiabilidad y solvencia muy alto, aunque sus resultados dependen fuertemente de la forma que hayamos elegido para la base de datos de usuarios.

Una cosa es clara: si hemos de pensar en resguardar los datos de los distintos sectores o subredes, centralizar el manejo de archivos es una solución altamente recomendable. La implementación de un servidor de archivos implica "ponerle la cereza" a un esquema de autenticación distribuido, ya que no representa una complicación, más allá de destinar un nodo de la red, y sumarlo como cliente de algunos servicios (como el tipo de autenticación), y como servidor de otros (NFS, SAMBA, etc.).

Canales seguros en un mundo inseguro

Un punto a considerar si es necesario realizar conexiones habitualmente con otros puntos externos a la red de la organización (sucursales, personal que trabaja desde su casa, etc.), y que deban utilizar el soporte de Internet para llegar hasta nosotros es la implementación de algún tipo de túnel seguro, o VPN. Hay varias soluciones disponibles, dependiendo de las necesidades y la escala de trabajo remoto a desempeñar. Si necesitamos conectarnos remotamente para mantener los servidores o la red, con un simple Gateway SSH podemos arreglárnoslas. Hasta podemos encapsular tráfico a un solo puerto sobre SSH, por lo que podríamos correr un servicio remotamente mediante este tipo de conexiones. Ahora bien, si debemos brindar conectividad a una intranet remota, debemos pensar en productos más potentes como OpenS/WAN u OpenVPN.

Surge así un nuevo interrogante: ¿Dónde colocamos el Gateway VPN? ¿Sobre uno de los firewalls de la VPN? ¿En la DMZ? ¿Fuera de ésta, incrementando el área de frontera expuesta? A la hora de decidirnos por colocar un punto de acceso VPN, si deseamos plantearlo sobre una plataforma Linux, deberemos pensar en destinar para él una máquina bastante potente, por cuanto la generación de túneles seguros es una gran devoradora de recursos. Lo ideal sería colocarlo detrás de uno de los firewalls principales, realizando reenvío de tráfico en el mismo a los puertos pertinentes. O, si disponemos de varios puntos de acceso a Internet en la frontera de nuestra red, podríamos pensar en incrementar la longitud de ésta frontera colocando en ella nuestro Gateway VPN.

Lo que es claro es que nuestro punto de acceso VPN no debería correr más servicios que el de generador de túneles seguros, y que su firewall debería estar configurado para dejar entrar desde el exterior sólo éste tipo de tráfico. Debería además poseer su propio esquema de autenticación de usuarios, o funcionar como mero cliente de un servicio interno de autenticación centralizada, pero en ningún caso debería poseer una copia de la base de datos de usuarios disponible para la Intranet.

Jugando al "Big Brother"

Como en la novela "1984" de George Orwell, en toda red debe existir un ente u organismo que vele por la seguridad de los usuarios, y que sea capaz de monitorear el tráfico en tiempo real. En una red pequeña ésto puede resultar posible, pero conforme escalamos hacia arriba, el volumen de tráfico y la complejidad del mismo hace necesario caer en productos que nos ayuden en esta tarea.

Más arriba comentábamos la necesidad de instalar HIDS (como TripWire o AIDE) en los servidores de la DMZ, y correr una versión de alguno de estos programas desde un CD, dispositivo USB o diskette. En general, no conviene crear la base de datos de estas aplicaciones sobre el sistema de archivos de los firewalls o servidores, ya que si un atacante gana acceso a ellos, lo primero que hará será regenerarla para esconder las modificaciones realizadas. Ahora bien, ¿Cómo monitoreamos la actividad de los clientes de la Intranet? Bueno, existen varias soluciones disponibles. La más simple -y de menos alcance- es instalar en los proxys de las distintas subredes un monitor de tráfico como Ntop. Una más compleja (y completa) es instalar en estos proxys *Snort*, un detector de intrusiones orientado a redes, integrarlo con una base de datos, con su frontend de acceso web *Acid*, y configurarlo para que nos reporte vía correo o SMS cualquier actividad anómala ocurrida en la red. Snort es -para usar un eufemismo muy de moda- "flexible, potente, y extensible". Traducido al castellano básico: no es como para principiantes. Al respecto, recomiendo una excelente nota de Pablo Gonzáles Mateos en el número de noviembre de 2005 de ésta misma revista.

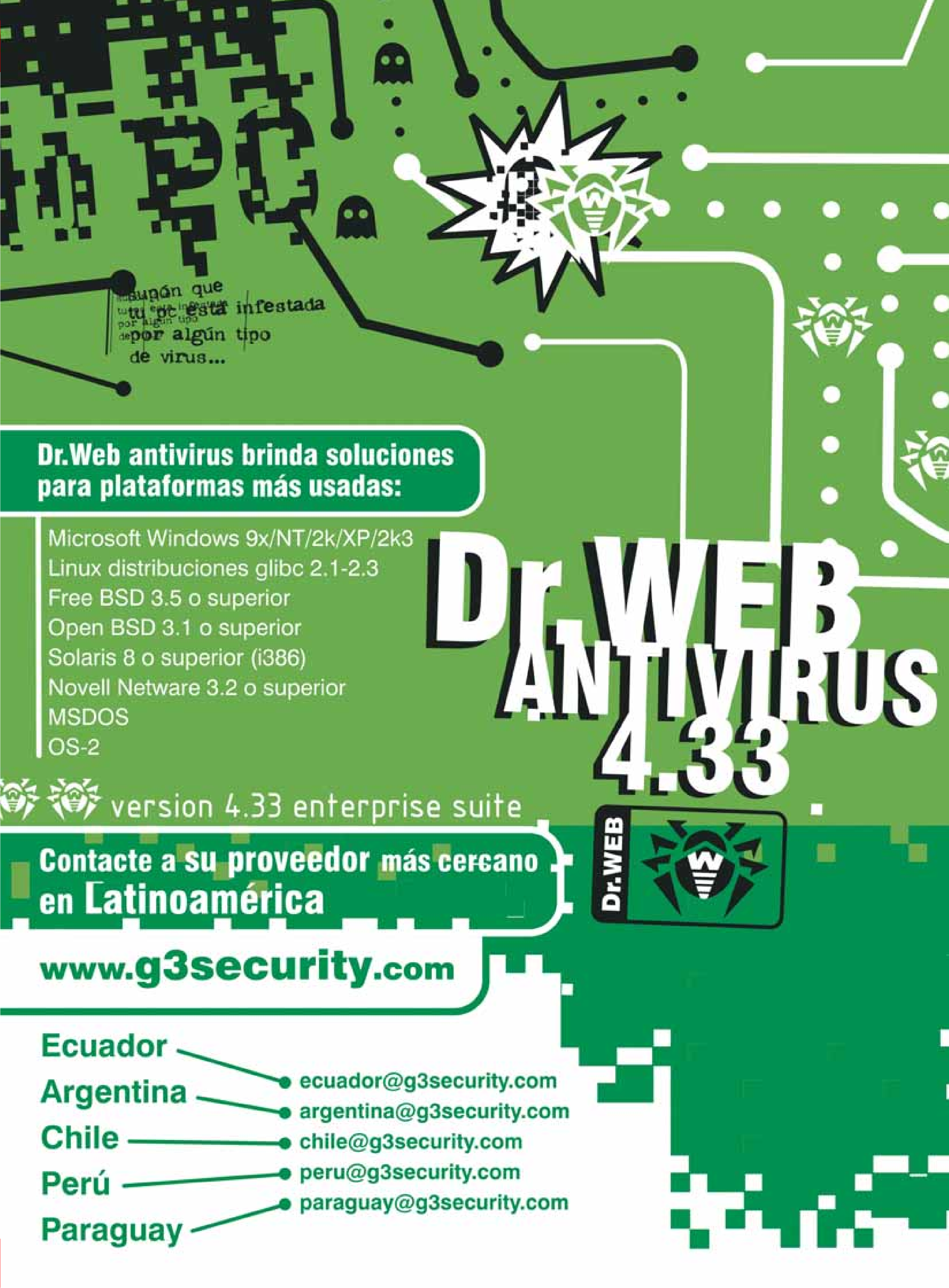
Otro punto a considerar es relevar las potenciales amenazas de seguridad. Para ésto, podemos desplegar Nessus en nuestra red de manera permanente, o utilizar una solución trashumante como ASC (ambos casos se hallan cubiertos en notas anteriores en esta misma revista). La dificultad de la segunda opción reside en que no podremos actualizar la base de datos de plugins a la última disponible en el momento de realizar el relevamiento. La única solución es descargar una nueva versión de la distribución ASC, con un listado de plugins actualizados. En cualquier caso, la evaluación de potenciales vulnerabilidades se debe realizar de manera periódica, por lo que deberemos pensar en ajustar un cronograma para estas actividades.

Un punto importante a considerar es el factor psicológico: relevar vulnerabilidades y analizar las alertas de un IDS se vuelve rutinario después de un tiempo. Y es muy fácil que esta rutina se nos haga pesada, al punto de dejar de prestarles atención a los mensajes de estos programas. Es necesario tomar conciencia de que, si bien hay altas probabilidades de que no suframos ninguna intrusión en toda nuestra vida como administradores -sea porque hemos trabajado bien, sea porque nadie se ha fijado hasta ahora en nuestros hosts-, lo más probable es que debamos enfrentarnos a algún intento de intrusión, o a algunos *script kiddies* tratando de averiguar datos sobre las vulnerabilidades presentes en nuestras redes. O aún peor, a algo más grande. Y cuando estas cosas pasen, sólo la constancia en el trabajo de actualizaciones, la reacción ante un alerta de vulnerabilidades por parte de un CERT, o lo abiertos que tengamos los ojos a un aviso de los IDS nos salvarán, y evitarán que lo que hemos construido se derrumbe… ■

Para seguir leyendo:

- *"Detección de Intrusos Bajo Linux" - Pablo González Mateos - NEX, noviembre 2005.*
- *Monitorización de tráfico de red: www.ntop.org*
- *AIDE - Advanced Intrusion Detection Environment: www.cs.tut.fi/~rammer/aide.html*
- *Detección y prevención de intrusiones: www.snort.org*
- *Análisis y detección de vulnerabilidades: www.nessus.org*
- *Introducción a Nessus: www.securityfocus.com/infocus/1741*
- *Las 75 Herramientas de Seguridad Más Usadas: www.insecure.org/tools/tools-es.html*





tu pc está infestada
por algún tipo
de virus...
Dr.Web antivirus brinda soluciones para plataformas más usadas:
Microsoft Windows 9x/NT/2k/XP/2k3
Linux distribuciones glibc 2.1-2.3
Free BSD 3.5 o superior
Open BSD 3.1 o superior
Solaris 8 o superior (i386)
Novell Netware 3.2 o superior
MSDOS
OS-2
Dr.WEB ANTIVIRUS 4.33
version 4.33 enterprise suite
Dr.WEB
Contacte a su proveedor más cercano en Latinoamérica
www.g3security.com
Ecuador
Argentina
Chile
Perú
Paraguay
ecuador@g3security.com
argentina@g3security.com
chile@g3security.com
peru@g3security.com
paraguay@g3security.com

Microsoft® TechNet

Alta disponibilidad con SQL Server 2005

Aumentar la disponibilidad del servidor en una base de datos es un deber y un gran dolor de cabezas que tienen la mayoría de los DBA.
En la mayoría de los casos cuando hablamos de alta disponibilidad son soluciones costosas y algunas muy difíciles de implementar y mantener.
Microsoft SQL Server 2005 ofrece unas baterías de opciones para esto, que permitirán hacer mas feliz la vida del DBA y a un costo/Beneficio excelente.

por **Maximiliano Accotto**

Antes de entrar en detalle sobre las opciones de alta disponibilidad en SQL 2005 haremos una breve introducción al tema. Primero debemos comprender que es alta disponibilidad.
Cuando hablamos de disponibilidad hacemos referencia a cuanto tiempo un servicio está disponible para su uso, ese tiempo lo debemos medir vs. el tiempo que debería estar funcionando ese servicio, por Ej.: si tenemos un servidor de base de datos que debe funcionar 7x24 y en el año tenemos una parada del servicio de 24hs entonces estaremos hablando que ese servidor tiene una disponibilidad de: 99,72% de su total de horas. Los valores de disponibilidad dependerán del negocio, habrá negocios donde se requiera un valor próximo al 100% y otros donde no sea tan necesario.
El servidor de bases de datos (SQL Server 2005 en este caso) es un servicio que será consumido por distintos clientes (aplicaciones, sistemas de reportes, etc.) y debemos asegurar que los clientes tengan el servicio lo máximo disponible.
Supongamos que estamos sirviendo en esa base de datos un servicio donde se conectan aplicaciones de un E-Comerce, todo el tiempo que esté fuera de servicio serán menos U$D de ingresos seguramente. Existe actualmente una medición llamada 5 nueves (9s) por el indicador de 99.999% del tiempo disponible de un servicio.
La siguiente tabla muestra los diferentes indicadores y el tiempo que debería estar fuera de servicio el servidor para cada uno de ellos.

Que nos ofrece SQL server 2005 para asegurar la alta disponibilidad

Esta versión de SQL Server nos ofrece los siguientes modelos para poder aumentar la disponibilidad del servicio.

- *Cluster*
- *Database Mirroring*
- *Log Shipping*
- *Replicación.*

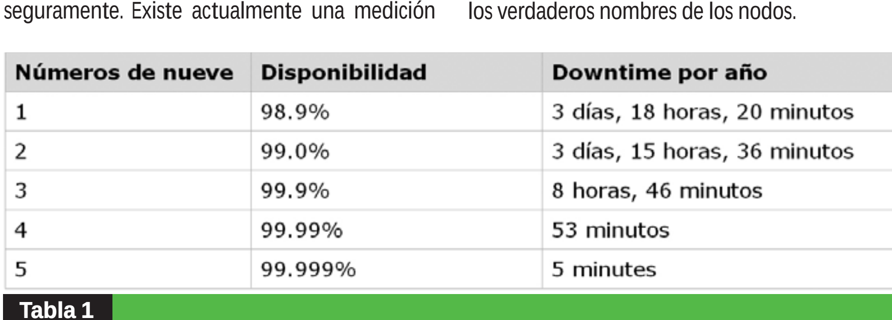
Clustering

El modelo Cluster de conmutación por error es la combinación de uno o más nodos (Servers) que disponen de dos o más discos compartidos.
SQL Server se debe instalar en cada uno de los nodos disponible y la combinación de ellos junto con el nombre de red y una dirección IP formarán lo que se denomina servidor virtual, el cual será conocido por las aplicaciones sin que éstas sepan los verdaderos nombres de los nodos.

El cluster de conmutación por error ofrece lo siguiente:
- *Conmutación por error manual.*
- *Conmutación y detección por error automático.*
- *Transparencia en la redirección de los clientes.*

Así como nos ofrece estas ventajas debemos conocer las siguientes limitaciones de este modelo:
- *No protege si hay errores de disco.*
- *Se aplica a la instancia del servidor*
- *Utiliza una sola copia de la Base de datos*
- *Requiere Hardware certificado*
- *No soporta la generación de informes en modo de espera*

El modelo de cluster está disponible para las versiones Enterprise, Developer y Standard de SQL 2005, esta última con una serie de limitaciones. La figura 1 nos muestra un modelo simple de Clustering.



Números de nueve	Disponibilidad	Downtime por año
1	98.9%	3 días, 18 horas, 20 minutos
2	99.0%	3 días, 15 horas, 36 minutos
3	99.9%	8 horas, 46 minutos
4	99.99%	53 minutos
5	99.999%	5 minutes

Tabla 1

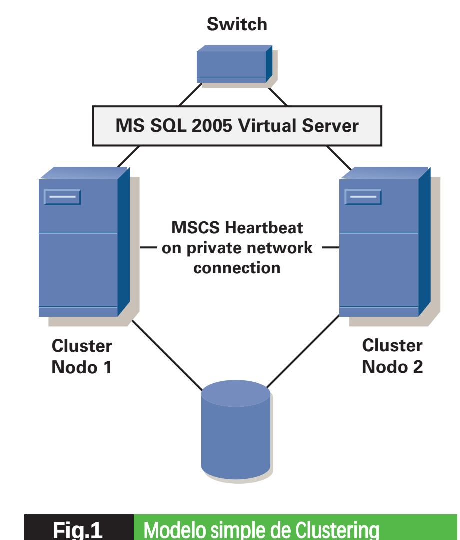


Fig.1 Modelo simple de Clustering

Mirroring

Mirror es una nueva opción que nos ofrece SQL 2005, esta solución de software está pensada para aumentar la disponibilidad de la Base de datos por medio de una gestión inmediata por la conmutación por error.

Esta configuración está compuesta por: un servidor principal, un servidor mirror y un servidor testigo como opcional. El servidor mirror es actualizado de forma constante y la conmutación por error es prácticamente instantánea.

La ventaja que tiene este método sobre el Log Shipping es que se trata de una configuración que no pierde datos (sin pérdida de datos) compatible con una estrategia de conmutación por error simple. Éstos son algunos tips con respecto a Mirror.

- Utiliza servidores Standard.
- Es aplicado en la base de datos.
- Cuando trabajo de forma sincrónica garantiza la no perdida de datos gracias a la confirmación con delay de la base de datos principal.
- Incluye opciones de informe limitados para el servidor mirror por medio de las instantáneas de base de datos.
- Se aplica por base de datos.
- Sólo se aplica a bases de datos con el modelo recuperación Full.
- No se puede hacer mirror sobre bases del sistema como: Master, Model, Msdb o Tempdb. La siguiente figura 2 ilustra el modelo

Mirror aún no está certificado en SQL2005 RTM, para los primeros meses de este año 2006 ya debería ser liberada la certificación. El modelo de mirror funciona en las versiones Enterprise y con algunas limitaciones en la versión Standard del producto.

La inclusión del servidor testigo es opcional, como hemos mencionado anteriormente y este puede llegar a ser una versión Express del producto ya que sólo se lo utiliza como un tercer referente a la hora de comprobar si un Server ha perdido conexión.

Una de las ventajas que también trae este modelo es que desde el lado del cliente si se llegara a caer el servidor principal no habría que cambiar cadenas de conexión que apunten al servidor mirror, para ello SQL2005 implementa junto con ADONET algunas mejoras en las cadenas de conexión, el siguiente ejemplo muestra como indicar en la cadena de conexión el servidor principal y cual seria el servidor mirror en caso de error.

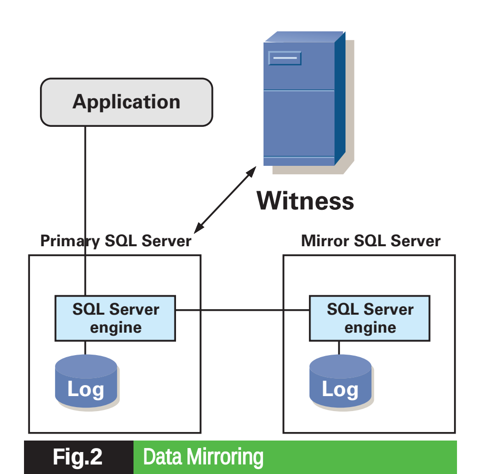


Fig.2 Data Mirroring

"server=Partner_A; failover partner=Partner_B; database=AdventureWorks"

Log Shipping

El logShipping al igual que el mirroring se aplica por base de datos. La configuración para este modelo incluye a un servidor primario uno o más secundarios y uno de supervisión (opcional). Los servidores secundarios son actualizados en intervalos de tiempos por las copias de seguridad de los registros del servidor primario (transaction Log), antes de producir la conmutación por error la base de datos secundaria se debe actualizar por completo de forma manual.

El servidor de supervisión es el que se encarga de monitorear y hacer un seguimiento del logShipping. Este servidor debe estar alojado en un servidor independiente con el fin de evitar la perdida de información y la función de supervisión si es que se pierde el servidor primario o secundario.

Este modelo esta disponible para las versiones Enterprise, Developer y Standard.

Replicación

La replicación es otra alternativa de alta disponibilidad, este modelo consiste en un publicador y uno o más suscriptores, esto permite que el publicador distribuya la información a cada uno de estos suscriptores. La réplica consta de las siguientes características:

- Permite más de una copia redundante de la base de datos.
- Permite una disponibilidad completa de los secundarios (suscriptores) que se podrían por Ej. utilizar para informes, etc.
- Se aplica a la base de datos.
-Asegura la escalabilidad y disponibilidad en tiempo real entre las bases de datos.

La opción de réplica está disponible para todas las versiones de SQL2005 excepto la Express y la Movile. La figura 3 muestra el modelo de replicación

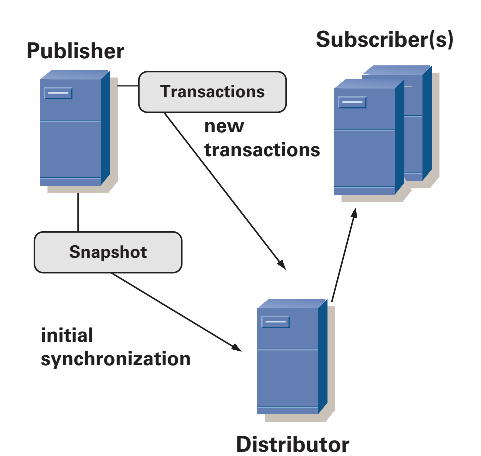


Fig.3 Modelo de Replicación

Conclusiones

Como hemos podido observar SQL2005 ofrece varias alternativas para mejorar la disponibilidad del servicio. La gran novedad en esta versión es sin dudas Mirroring que aunque hasta el día de hoy no este certificado en las pruebas que he realizado ha funcionado bien. La tabla 2 muestra las comparativas entre modelos.

Maximiliano Accotto:



Gerente de Sistemas en Fundición San Cayetano S.A. y flamante Microsoft MVP en SQL Server. Desde el año 1992 se dedica al análisis (desarrollo), gestión y mantenimiento en el mundo IT , utiliza Microsoft SQL Server desde la versión 6.5 en distintos sistemas corporativos.

Posee una amplia experiencia en sistemas ERP, CRM, dirección de proyectos, análisis tecnológico, base de datos, arquitectura de sistemas corporativos y lenguajes de programación .Tiene 3 estrellas del programa Desarrollador Cinco Estrellas y participa activamente en los news de Microsoft y foros del MUG además de escribir artículos para los sitios de interés en SQL Server.

Attribute	Clustering	Log shipping	Database mirroring
Detección de Falla	Si	No	No
Failover Automático	Si	No	Si
Tiempo de Downtime percibido	30 segundos + recuperación	N/A	3 segundos
Potencial "data loss"	Si - una copia de data	Si - ultimo log de transacción	Si - en algunas configuraciones
Masking of storage failure	No - Disco compartido	Yes	Yes
Hardware Special	Storage y Servidores Certificados	No	No
Distancia	100 millas	Ilimitado	Ilimitado
Scope	Systema y Bases de Datos de Usuarios	Datos de Usuarios	Datos de Usuarios

Tabla 2 Comparaciones entre modelos



¿Qué es un Site Survey?

Ing. Carlos Alberto Spera
IT Consultant Leader
Mundo del Soporte
Latin América

Con el crecimiento sostenido que viene llevando la tecnología wireless - y en consecuencia las redes Wi Fi - , se torna imprescindible realizarlas bajo un método profesional, en cuyo contexto aprovechar las bondades de una herramienta, como el caso de Airmagnet y/o otras, garantizarán un output eficiente en cada implementación.

Una buena definición para *"Site Survey"*, puede ser: *"Mapa de red wireless satisfactoriamente implementada"*
Un Site Survey es el proceso de identificar y detectar las diferentes redes wireless que se encuentran en la cercanía de donde pensamos realizar nuestra implementación y poder así seleccionar el lugar estratégico para instalar nuestros equipos de manera de asegurarle a nuestros clientes una conveniente cobertura en los espacios por ellos elegidos.

Recomendaciones Básicas

Se debe tener en cuenta que un Site Survey es lo mas importante en la implementación de una red wireless.
Esta puede tardar días o semanas según la envergadura del proyecto, pero nunca se deberá obviar este paso ya que tal como refiero anteriormente resulta requisito "excluyente" a la implementación satisfactoria de una red wireless.
Resulta "objetivo primario" de un Site Survey el que todos los usuarios móviles puedan utilizar la red wireless siéndoles a la vez transparente su desplazamiento dentro de las instalaciones donde implementemos dicha red.

Preparándonos para un Site Survey

El planeamiento de una red wireless incluye la recolección de información y la toma de decisiones. Aquí algunas básicas que no deberían obviarse antes de comenzar cualquier Site Survey.
Las mismas pueden ser generalmente respondidas por el Administrador de la Red o bien por alguna persona idónea del sector de It.
- Tipo de estructura o Facility - Importancia
- Redes existentes (Ethernet, Wireless, Etc.)
- ¿Qué propósito tiene la red? (comercial, cortesía, otros)
- ¿Qué requerimientos en cuanto a roaming y ancho de banda será necesario ?
- ¿Qué recursos existentes están disponibles? (Tipo de conexión a internet, cableado, Etc.)
- ¿Cuáles son los requerimientos de seguridad? (mínimos, máximos).

Tipo de estructura Facility - Importancia

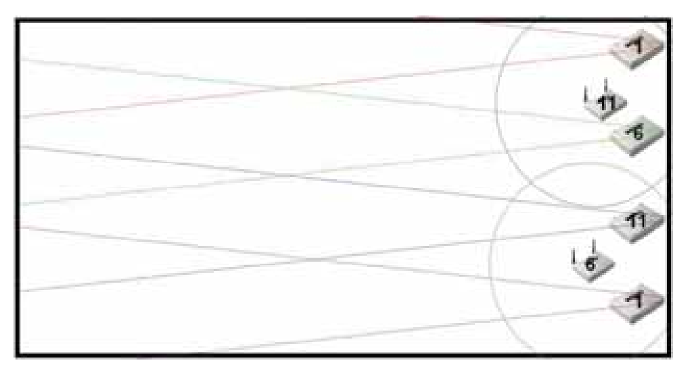
Es muy importante determinar a priori el tipo de estructura en la cual realizaremos el Survey ya que no es lo mismo realizarlo para una oficina con veinte (20) usuarios móviles que para un aeropuerto internacional que puede tener mas de doscientos (200) a la vez de asegurar una mayor área de cobertura.
Para ello, no solo se deberá cuantificar la diferencia en número de clientes concurrentes, si no también aquellos elementos de seguridad tal que garanticen el funcionamiento conforme al alcance esperado. Las respuestas a estas preguntas pueden venir en descripciones escritas, fotos, planos estructurales del edificio. Se debe considerar que cuanto más se profundice en el relevamiento previo -antes de llegar al edificio en cuestión- , estaremos mucho mejor preparados y ello nos facilitará obviamente, la tarea a realizar.-
Tomaremos como ejemplo para este caso ejemplo la estructura de un hospital.
En un site del tipo "hospital", deberemos considerar que varios factores ajenos a la lan, podrán afectar a nuestra señal de 2.4 Mghz. Equipos de radiología, de radio comunicación, ventanas malladas, puertas de seguridad, largos de pasillos, salidas de incendio, ascensores, materiales que componen las paredes, ladrillo hueco, concreto, durlock, Etc. .-
Todos ellos juegan un rol importante en cuanto a la expansión de señal.

Muy Importante

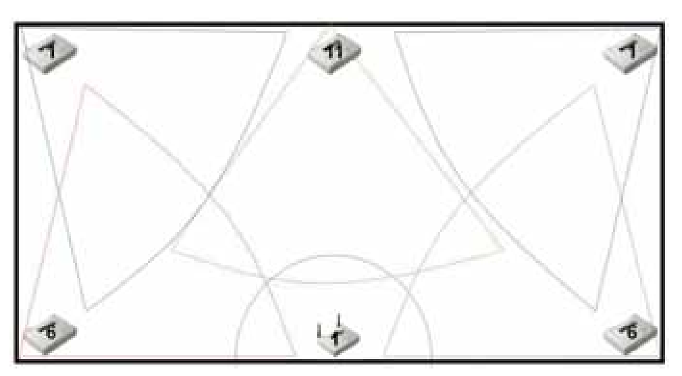
Antes de empezar a realizar cualquier actividad dar una vuelta completa a todo el site determinando el tipo de estructura (escaleras, ascensores, pasillos), materiales de las paredes, posibles interferencias así como ir analizando posibles puntos de montaje, explorando la forma de llegar con cable al punto elegido.

Deberemos tener en cuenta la utilización de dife-

	802.11b	802.11a	802.11g
Frequency Band	2.4 GHz	5 GHz	2.4 GHz
Availability	Worldwide	US/AP	Worldwide
Maximum Data rate	11 Mbps	54 Mbps	54 Mbps
Other Services (Interference)	Cordless Phones Microwave Ovens Wireless Video Bluetooth Devices	HyperLAN Devices	Cordless Phones Microwave Ovens Wireless Video Bluetooth Devices



Instalación de un warehouse con posibilidad de cablear alrededor del mismo. Importante la disposición de los canales.



Instalacion de un warehouse con solo la posibilidad de cablear sobre una pared. Usando antenas Omnidireccionales y Yagui.

rentes tipos de antenas (direccionales u omnidireccionales) dependiendo por ejemplo de si corresponde resolver un pasillo o una sala de espera, Etc. , todo lo que facilitará la gestión de señal, siempre que sea convenientemente utilizado.
También, en un Survey de este tipo, deberá considerarse la creación de diferentes SSID para visitantes o bien para uso del personal interno, con roaming automático.
Se deberá además efectuar un cálculo estimado de la cantidad de usuarios que se puedan conectar a los diferentes Access Point por el ancho de banda y perfomance.
Estas son algunas de las consideraciones a tener en cuenta en este tipo de site.
Otro ejemplo diferente puede ser de una estructura tipo open office como hoy en día son la mayoría de los contacts center´s, sin grandes divisiones, todas estructuras bajas tipo box, con la mayoría de las paredes de durlock o paneles y con una cantidad de veinte (20) o más usuarios móviles y fijos.
Son estructuras generalmente libres de obstáculos donde la señal se propaga fácilmente. Aquí es importante tener en cuenta la cantidad de usuarios que van a estar conectados en forma concurrente debido a la necesidad de establecer el ancho de banda tolerado para el perfil de usuario móvil, que usualmente ocupa 80 % Internet (Navegación - Mail) y 20% transferencia de pequeños archivos del file server.
En cuanto al ítem de seguridad, convendrá establecer adecuadamente los accesos a los diferentes Servers, implementar subredes, roaming automático, diferentes SSID para visitantes, Etc. (Ver Seguridad).

Redes existentes (Ethernet / Wireless)

Es éste un punto clave en la definición estratégica de la lan, ya que con esto sabremos si convendrá montar una red que deba coexistir con otra existente o bien si deberemos realizar el diseño desde cero.
Muchas veces nos vamos a encontrar con redes wireless ya implementadas, en cuyo caso deberemos realizar algunas preguntas extras, a saber:
- Documentación de la red existente
- Frecuencia y canales que se están utilizando
- Cantidad aproximada de usuarios
- Tipo de seguridad implementada
- Sectores del site que presentan en facilidad wireless y cual cableada
- Equipos que se están utilizando (Access Points, switches, hubs, routers, modems) y donde están localizados.
- Tipo de roles de los AP´s instalados (root, repeaters, bridges).-

Sin estas consideraciones, el site survey será mucho mas complejo, sobretodo si la red existente no hubiera sido implementada correctamente.

¿Qué propósito tiene la red? (Comercial - cortesía)

Se debe establecer a priori -y hacerlo correctamente- , el uso que el cliente dará a la red wireless. Solo de esa manera podremos realizar un planeamiento preciso tanto en cuanto a la configuración como en lo referente al hardware a utilizar. Todo lo cual redundará en un proyecto económicamente viable y muy posiblemente; exitoso.

¿Qué requerimientos en cuanto a roaming y ancho de banda?

Una vez mas esto depende del uso que el cliente le vaya a dar a la red. Por ejemplo: Si se presenta un cliente en cuyo caso la red wireless será el vínculo para una aplicación que transmita códigos de barras de las cajas del depósito al Server central con un ancho de banda de (3 - 5 Mbps.), puede resultar satisfactorio, no obstante seguramente más importante aún resultará que el roaming esté activo en todo el depósito de manera que el casual operario se pueda mover con libertad sin restricciones evitando estar pensando si está o no conectado.
Una situación diferente sería si nos encontramos con una oficina de operadores que trabajan bajo web, los que necesitan acceder a pesadas bases de datos y/o testear a la vez el rendimiento de servers -sea que estos se encuentren siempre en la misma área de trabajo o no-. Aquí lo mas importante es el ancho de banda que seguramente van a estar necesitando el que será no menor a (48 - 54 Mbps.) y va entonces a tener menos importancia el tema del roaming ya que no van a estar pasando de una red a otra.
A tener en cuenta:
- Cantidad de usuarios que van a estar conectados a la red.

Dependerá de la cantidad de usuarios que se conectan a la red wireless el ancho de banda del que van disponer, por eso ese dato debe ser lo mas preciso posible.
- Tipo de aplicaciones van a estar corriendo sobre la red wireless.

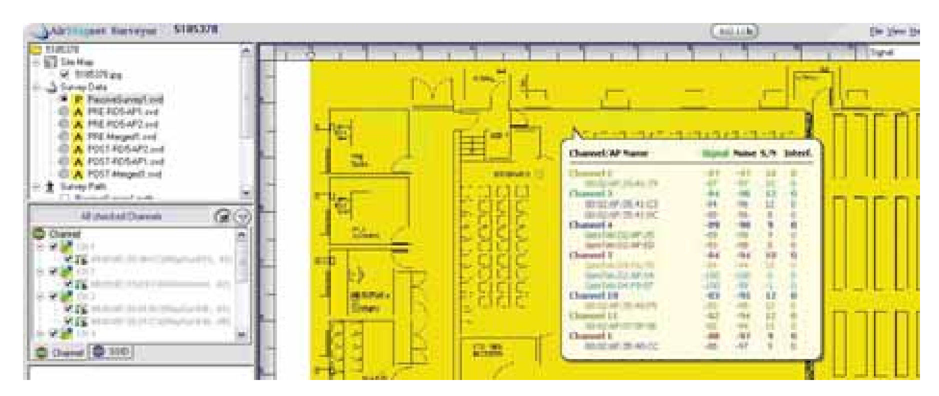
Resultará factor clave medir el tráfico de paquetes.
Dependiendo de las aplicaciones que corran y en que área (sala de reuniones, zona de oficinas, Etc.) se puede dar prioridad a ciertos paquetes para asegurar una buena comunicación (tasa de transferencia).
- Roaming de los usuarios

También se debe determinar que usuarios van a tener roaming ya sea dentro de un edificio, departamento o bien se puede considerar que dispongan roaming en todas las sucursales.

¿Qué recursos tenemos disponibles?

Este punto nos puede alivianar mucho trabajo. Debemos recolectar la mayor cantidad de información disponible solicitándosela al administrador de la red.
Esta consistirá en: planos estructurales del edificio, documentación de un site survey previo, documentación de la topología de la red actual, Etc. .-
Deberemos considerar el franqueo a lugares de acceso restringido, solicitando permiso previo para ingresar en esas áreas.
También deberíamos tener en cuenta si hay una red wíreless instalada qué marca son los equipos, qué Frecuencia son, qué tipo de antenas están usando y dónde y cómo están instalados.
Además debemos tener claro con cuanto tiempo disponemos para realizar el Site Survey y por últi-

	900 MHz	2.4 GHz	5 GHz
PROs	Greater Range than 2.4 GHz (For in- Building LANs)	Global Market IEEE 802.11 Higher Data Rates (10+ Mbps)	Global Market IEEE 802.11 Higher Data Rates (20+ Mbps)
CONs	Maximum Data Rate 1 Mbps Limited Bandwidth Crowded Band	Less Range than 900 MHz (For In-Building LANs)	Much Less Range than 900 or 2.4GHz Higher Cost RF Components Large Antenna required



Pantalla de Passive survey. Se puede observar qué redes entrantes hay separadas por canal y además da la información de que fuerza de señal esta ingresando. Eso se puede ver en cualquier punto del plano solo moviendo el Mouse.

mo pero no menos importante con que presupuesto cuenta nuestro cliente para realizar el trabajo.
Todo lo cual nos dará la pauta de si tendremos que planear la red con los equipos existentes reubicándolos o bien si disponemos de la posibilidad de realizar un cambio total de equipos.

¿Qué nivel de seguridad es necesario?

Frecuentemente los clientes van a querer asegurar la consistencia de la red tanto desde el aspecto lógico como físico.
En tal sentido es conveniente detallarle al mismo todas las opciones disponibles a fin de que juntos puedan evaluar la mejor alternativa.-
Ello podría extenderse desde la definición de seguridad bajo WEP hasta la autentificación de un servidor Radius.
En todos los casos es aconsejable detenerse en las ventajas y desventajas de los diferentes métodos así como en la posibilidad de sumar algún software extra de control global de APs o bien de un IDS especifico para la red wireless.
Eventualmente nos podemos encontrar con corporaciones y/o empresas multinacionales que disponen de políticas de seguridad global para la implementación de redes wireless.-
En ese caso deberemos solicitar al administrador de red, dichas normas para poder analizarlas detenidamente y evaluar si los equipos elegidos soportarán el tipo de seguridad definida o bien si la topología de red será la adecuada, Etc. .-

Conclusión

Habiendo visto ya todos los puntos en detalle podemos armar un check list que nos ayudará a recordar cada paso:

Check List de Site Survey

1) Planos estructurales del site.
2) Documentación de un site survey anterior.
3) Documentación y diagrama de la red (topología).
4) Programar una reunión con el administrador de la red.
5) Programar una reunión con gente de mantenimiento del site (arquitecto, administrador de propiedad).
6) Asegurarse acceso a todas las áreas donde vamos necesitar chequear la señal wireless.
7) Acceso al rack central o N.O.C.
8) Acceso al techo, descendido para ver posibles puntos de montaje (escalera).
9) Informarse de futuros cambios de estructuras, ampliaciones y mudanzas de oficinas.

Herramientas

Existen en el mercado novedosas "armas" que nos permiten optimizar la gestión de diseño e implementación de una red wireless.-
Con ellos lograremos un trabajo mucho más profesional y eficiente, garantizándole a la vez a nuestro cliente que ha escogido el camino más adecuado.
Entre otras empresas que han dedicado valiosos esfuerzos a esta etapa de un site wireless, se destaca la empresa Airmagnet, quien presentó una tool, que denominó "Survey".
Este programa nos permite importar un plano del edificio o planta donde vamos a realizar el site survey el que una vez digitalizado y reconocido, nos facilita enormemente la toma de mediciones del lugar en forma cierta, las que luego se trasladan al programa dando como output un layout de espectro con altísimo nivel de certidumbre.
Como primer paso vamos a realizar un "Passive Survey". Esto significa que vamos a estar captando todas las señales entrantes (ajenas o internas) del área donde nosotros estamos caminando. De esta manera nos permite saber de donde vienen y con que fuerza están entrando las señales, en qué canales, qué tecnología a, b o g y ssid (en el caso que sea broadcasting) y en el caso que no vamos a ver la MAC address del dispositivo.
Para un correcto aprovechamiento de la herramienta, es recomendable caminar "bien" todo el perímetro del edificio, de forma tal que podamos captar la mayor información posible que después nos va ayudar a tomar decisiones a la hora de instalar los equipos.
Solo una vez cumplido este paso, debemos analizar la información.
El programa nos va a mostrar en que áreas se encuentran las señales entrantes, con que fuerza están ingresando el edificio y -muy importante- , en qué canal se encuentra la misma.
Esto nos permitirá a nosotros saber que canales puedo utilizar para poder evitar el overlapping con los canales entrantes.
Una vez que sabemos que canales tenemos disponibles para usar -siempre hablando dentro de la frecuencia 2.4 Mghz.-, el set de canales que no tienen overlapping son 1, 6 y 11.
Ejemplo: Si tenemos señales entrantes del canal 6 en todo el edificio provocados por access points vecinos y nosotros disponemos de dos access point´s, los canales que deberemos elegir para nuestros dispositivos resultarán el 1 y el 11; de esta manera evitaremos el overlapping.

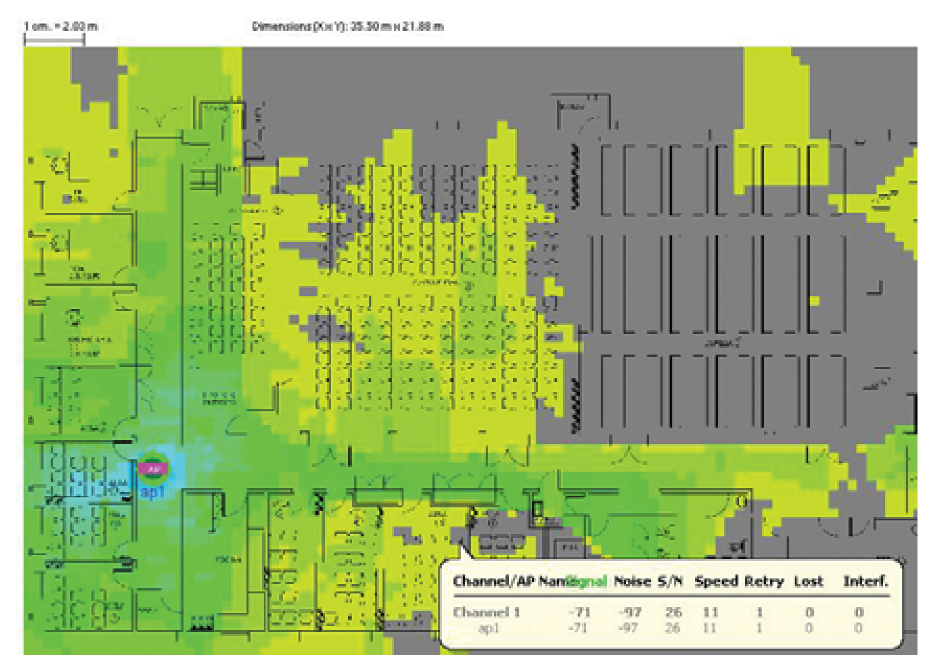
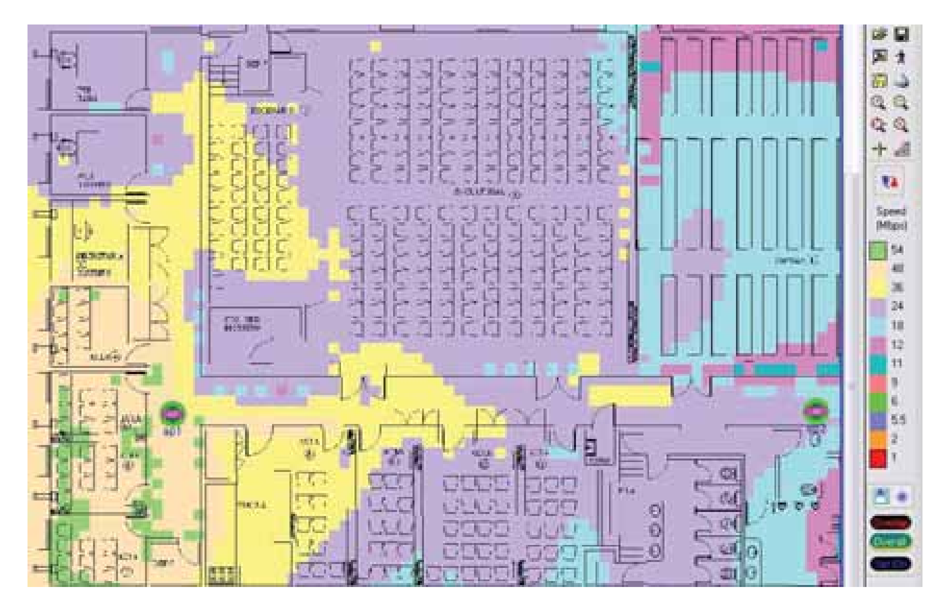


Imagen de Active Survey aquí podemos ver la senal que genera el Acces Point instalado (AP1) moviendo el Mouse por la pantalla vamos teniendo los valores como senal, velocidad, ruido, perdidas y mas.

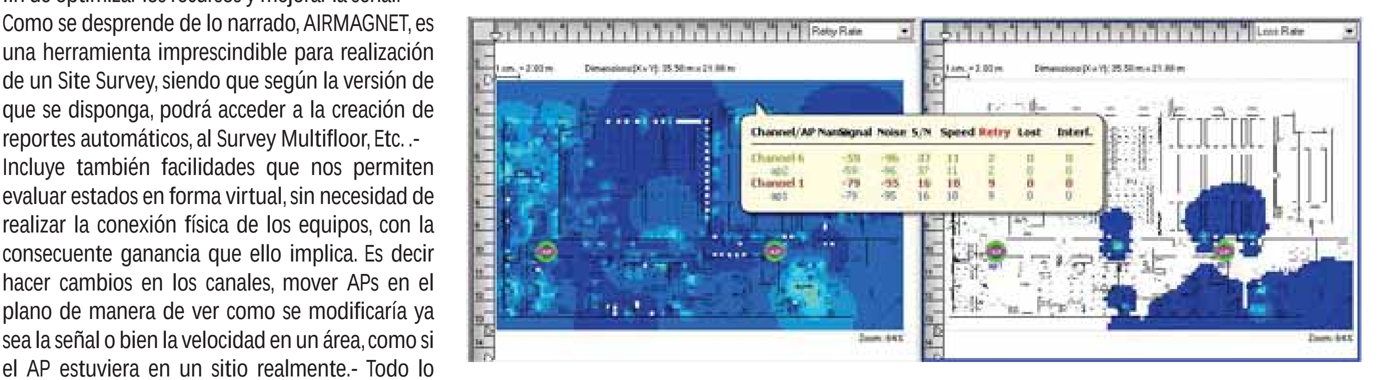
Luego de terminar de analizar esta información es hora de instalar los equipos para poder pasar a la segunda parte del Survey.
Procuraremos seleccionar puntos de montaje estratégicos a fin que nunca las antenas del tipo omnidireccional queden dispuestas en forma paralela a la pared.
Recomiendo para largos pasillos utilizar antenas direccionales tipo "patch" y para salas de reuniones o lugares amplios, antenas omnidireccionales.
Una vez que seleccionemos el predio y seteemos el canal deseado, vamos a realizar un Active Survey.
Este tipo de survey es muy diferente y tal vez el mas interesante ya que el programa nos permite enlazarnos con el access point. Así, mientras recorremos las instalaciones, vamos marcando en el plano que se encuentra en nuestro programa, por donde nos encontramos, a la que vez que recolectamos información y testeamos continuamente el AP.
Deberemos recorrer toda las instalaciones o la parte que debemos cubrir con señal sin olvidarnos que a la vez que caminamos deberemos ir señalando en el plano por donde estamos exactamente.
Una vez terminado el recorrido vamos a poder nuevamente ver la información recolectada.
Este tipo de survey nos va brindar un plano de señal donde vamos a poder ver que intensidad tiene la señal en las diferentes oficinas a la vez que nos permitirá tener un plano de velocidad de cada zona.-
Accesoriamente nos va a mostrar los lugares en donde se presenta pérdida de datos, cual es donde tenemos la mayor parte de reenvios de paquetes - si tenemos interferencia con canales - Todo esto lo marcaremos en el plano que hayamos cargado, lo que podrá guiarnos centímetro a centímetro acerca de qué sucede con nuestra señal, con qué velocidad llega a sala de reuniones, qué pérdida de paquetes tengo en el área de recepción, si tengo en algún punto del establecimiento interferencia con otros canales, Etc.
En cuanto a este tipo de Survey, debería confeccionarse uno para cada access point que vayamos a instalar ya que después, el programa nos permite realizar lo que se llama un "data merge" .-
Eso nos servirá para poder ver todla información de manera consolidada, o sea, los diferentes access points en un mismo plano, de forma que podremos determinar que área cubre cada dispositivo, si podemos correr un AP más cerca de un área, Etc. , a fin de optimizar los recursos y mejorar la señal.-
Como se desprende de lo narrado, AIRMAGNET, es una herramienta imprescindible para realización de un Site Survey, siendo que según la versión de que se disponga, podrá acceder a la creación de reportes automáticos, al Survey Multifloor, Etc. .-
Incluye también facilidades que nos permiten evaluar estados en forma virtual, sin necesidad de realizar la conexión física de los equipos, con la consecuente ganancia que ello implica. Es decir hacer cambios en los canales, mover APs en el plano de manera de ver como se modificaría ya sea la señal o bien la velocidad en un área, como si el AP estuviera en un sitio realmente.- Todo lo cual, con solo un "click" de mouse.



La imagen muestra la distribución de la velocidad después de instalar dos APs en el site. En el margen derecho esta la referencia.



Imagen del data merge después de realizar dos active surveys uno por cada cada AP instalado. El programa nos permite juntar las dos info para poder tener una vision completa de cómo queda el site.



La imagen muestra el Retry rate y el Loss rate de cada AP instalado.

Paneles de Hosting



Observando la amplia temática del hosting, los paneles de control cobran cada vez más importancia y justificación. Presentamos una introducción a los mismos y a su constitución dentro de su ámbito de funcionamiento.

Ing. Edgardo Daniel Lázaro
Dpto de desarrollo ferozo.net

Introducción

Abordaremos la temática del software denominado panel de control de hosting, a partir del proyecto ferozo (principalmente de su versión Linux), uno de los pioneros dentro de los paneles nacionales.
Como sabemos, el servicio de hosting se trata del alojamiento de las páginas web que gestionan empresas especializadas. Las empresas que se dedican a este servicio son como los hoteleros de la red: ofrecen espacio para que otras compañías almacenen cualquier información que quieran que sea accesible por una red, desde sus páginas web hasta la información de su red interna y sus casillas de correo. Siguiendo con este ejemplo, los paneles de control de hosting vendrían a ser en la web, algo así como los conserjes y el servicio de cuarto de nuestro ejemplo.

Software para servidores de hosting

Como ya podemos apreciar, la temática del hosting es amplia y en esta oportunidad dejaremos de lado lo que respecta a conectividad, hardware e infraestructura de red, y nos concentraremos en los servidores para hosting y más puntualmente en el software que éstos utilizan.
Para tener una idea más precisa de las necesidades que cubren los paneles de control y el motivo de su existencia, diremos que hablando de servidores para hosting hay 3 necesidades básicas:
1- Aplicaciones que proporcionen los servicios esenciales propiamente dichos del negocio (servidor web, scripting, servidor de correo, servidor de ftp, Motor BD, etc).
2- Aplicaciones capaces de administrar a los servicios anteriores y a sus usuarios.
3- Aplicaciones que permitan a los usuarios finales administrar la porción de los servicios y recursos que utilizan.
Los paneles de control de hosting son soluciones integradas que cubren una o más de estas cuestiones. En nuestro caso, ferozo cubre las tres.
Respecto de la primera de las necesidades, notaremos que muy generalmente, la función de los paneles de control se limita a proporcionar los paquetes instaladores de las aplicaciones que corren los mencionados servicios básicos del servidor de hosting. Adicionalmente, como en el caso de ferozo, el panel de control al instalarse, instala también todas las aplicaciones de servicios que el servidor de hosting requiere para cumplir su cometido: MySQL como motor de base de datos, servidor de web apache, exim como servidor de smtp, servidor imap courier, servidor de ftp proftp, etc.
En lo que al desarrollo del panel de control concierne, esta etapa es la dedicada al instalador de la aplicación, que además de instalar al panel propiamente dicho, se encarga de que queden funcionando en el servidor todas aquellas aplicaciones que brindan servicios troncales para el hosting y además configura el sistema para que estos servicios se inicien cada vez que lo hace el servidor. Ahora llega el turno de tratar nuestra segunda y tercera necesidad en un servidor de hosting, o sea de una aplicación capaz de administrar a los servicios y a sus usuarios y aplicaciones que permitan a los usuarios finales administrar la porción de los servicios y recursos que utilizan. Acá es donde comienza a entrar en juego el panel de control de hosting propiamente dicho.



Ventajas de operar con un panel de control

Por supuesto, es verdad que se puede proveer a usuarios del servicio de hosting sin utilizar un software de panel de control. Pero esto, es viable sólo si el volúmen de usuarios del servidor es pequeño. En estos casos, cada requerimiento de un usuario del servicio tendría que ser atendido "manualmente" por el administrador del sistema, desde la creación de su cuenta hasta cada modificación o anexado a la misma, como crear o borrar una cuenta de email, o de ftp; crear una base de datos o un usuario del motor de BD, cambiar un password, brindar información estadística, etc.
Se comprenderá que ésto, con grandes volúmenes de usuarios en un servidor, demandaría demasiado tiempo de trabajo del administrador del servidor. Y ni pensar en disponer de multitud de servidores a administrar. Atender esta cuestión es la principal razón de ser de los paneles de control.



Descripción de la constitución de un panel

El panel de control de hosting es un software que se utiliza principalmente por tres niveles de usuarios:

- *Administrador del servidor o "root"*
- *Revendedores*
- *Usuarios finales*

Este hecho, en el caso de ferozo, delinea las interfaces o front-end.

Una interfaz es la que usan los niveles de usuarios Administrador del servidor y revendedores. Mediante su uso, pueden realizar acciones que son englobadas dentro de:

* Creación, modificación y eliminación de cuentas. Por ejemplo un administrador o un revendedor puede, por intermedio del panel, dar de alta, de baja o modificar una cuenta de hosting de un usuario, suspenderla, etc.

* Administración y restricción de recursos de cada cuenta, Como habilitarle cierta característica como capacidad cgi; cambiarle parámetros de la cuenta como quota y transferencia; modificarle una zona dns, comprobar el estado de los servicios que corre el servidor.

La otra parte de la que se compone el panel es una interfaz para usuarios finales. Mediante la misma, los usuarios pueden cambiar parámetros de su cuenta, como passwords e idioma; crear cuentas de correo, ftp, etc; crear usuarios y bases de datos en el motor de BD; instalar un contador de visitas o aplicaciones enteras pre-empaquetadas de libre distribución en su página, etc.

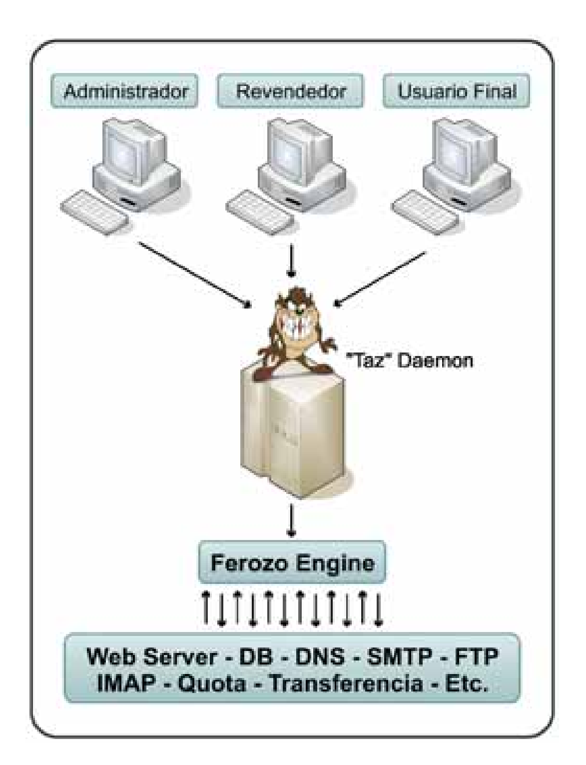


Atendiendo ahora lo que al desarrollo del software concierne, en lo que a la interfaz respecta, las consideraciones no son muy diferentes a las que se tienen en cuenta en otros tipos de software. Quizás la más importante característica sea la separación entre la presentación y el contenido. En nuestro caso, ferozo logra este objetivo mediante el uso de plantillas XSLT y los resultados son obtenidos mediante la transformación de los datos provistos por un documento XML, que es creado por las capas de comportamiento y negocios.

Esta características permite a la presentación, entre otras cosas, cambiar de idioma, de skin, personalizar, etc, de forma eficiente. Y lo que es de importancia para el equipo de desarrollo, la separación de tareas entre diseñadores gráficos y diseñadores de software propiamente dicho, los diseñadores de interfaces y procesos, y programadores.

Pasemos ahora a otro tema que respecta al desarrollo del software que tratamos: la arquitectura.

Ferozo, en su versión Linux, está construido utilizando una arquitectura cliente - dispatcher o de broker operacional. El motivo para esta decisión está en que, por un lado, es necesario que los componentes de presentación e interfaz corran sin más permisos que los necesariamente bastante limitados que tiene el servidor de web, y por otro, que desde las peticiones que se generan desde la interfaz se disparen cambios más o menos importantes en el servidor de hosting, como lo son el agregado de un usuario, reinicio de servicios, agregado de zonas de dns, etc.



De esta forma, las operaciones que necesitan privilegios especiales para ejecutarse, como las que se realizan sobre los servicios que corre el servidor o el acceso a carpetas restringidas del sistema de archivos, son llevadas a cabo por el broker. El broker es, en este caso, un proceso que corre como daemon o servicio, que crea un subproceso para atender a cada petición hecha desde los componentes del front-end y obtiene los permisos suficientes para ejecutar la acción una vez validada la petición.

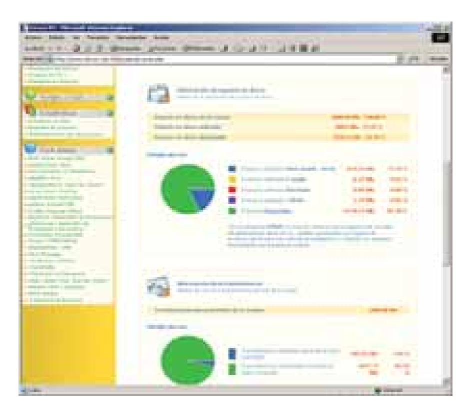
Otra de las decisiones importantes en el desarrollo de estos productos, como en la de cualquier otro, es la de los lenguajes de programación a utilizar. La interfaz gráfica con el usuario está enteramente programada con PHP, un lenguaje pensado para ser embebido en páginas web, flexible, que brinda toda la funcionalidad requerida del caso.

El daemon de ferozo está programado en c, debido a la eficiencia necesaria para un broker que debe atender cientos de peticiones por hora.

Los componentes de funciones específicas (engine) que ejecuta el broker, están escritos en c, python, php y bash. El criterio para la elección del lenguaje en estos últimos casos fue un balance entre performance y facilidad de construcción y mantenimiento, que obviamente varía según el caso.

Algunas particularidades de Ferozo

Pack-Amigo: Consta de un conjunto de aplicaciones populares pertenecientes al software libre, que se instalan automáticamente, mediante el panel, en la carpeta pública de la cuenta del usuario final que la requiere, sin necesidad de descargar el instalador, ni hacer ningún tipo de configuración. Así si, por ejemplo, el usuario quisiera para su sitio una tienda virtual, podría tener instalado con sólo especificar la carpeta destino, una aplicación e-Commerce como el os-Commerce.



Acceso webmail: Cada usuario de una casilla de correo, como alternativa a utilizar clientes locales de correo pop3 o imap, tiene disponible un acceso webmail a su cuenta de correos desde virtualmente cualquier parte.

Restricción y suspensión de usuarios: Las cuentas de usuarios finales están restringidas en el uso de recursos, como ser la cantidad máxima de cuentas de email que puede crear, la cantidad máxima de cuentas de ftp, la cantidad máxima de bases de datos en el motor. Así mismo, el panel es capaz de medir y con esta información suspender a un usuario excedido en la cantidad máxima de transferencia que puede utilizar.

Accesos temporales: Esta capacidad consta de facilitar acceso público a un sitio web cuando el dominio del mismo no puede ser resuelto por nombre por el servidor que lo aloja, por cualquier motivo. Ya sea que el dominio no está delegado al servicio de nombres que usa el servidor del hosting o simplemente se carece de un nombre de dominio. Esta característica hace uso de una propiedad del servidor de web, que permite acceder a la carpeta pública de cada usuario, a través de su nombre.

Conclusión

La principal problemática de los servidores para hosting está dada por cómo compartir recursos limitados entre numerosos usuarios. El panel de control de hosting resuelve en gran parte esta situación y juega un papel de vital importancia en optimizar los recursos compartidos y en limitar a los usuarios en la utilización de los mismos.

BREVES

Ubuntu en la escuela

En la edición #21 (pág. 78) de NEX IT Specialist hablamos sobre esta completísima distribución de Linux, e incluso acerca de su creador en esta misma sección en la edición anterior. A las ya conocidas versiones para 32 bits, 64 bits, y Mac, se les suma una nueva variante. Edubuntu es una distribución destinada al uso escolar, y a pesar de ocupar un solo CD, cuenta con herramientas adecuadas para su implementación dentro del aula (más de 16000 aplicaciones); usa Gnome 2.12, que permite una instalación rápida y fácil. Edubuntu es apto tanto para PC de escritorio como para su uso en servidores ya que incluye el Linux Terminal Server incorporado. La versión actual (5.10) soporta las arquitectura de microprocesadores Intel x86 (y PCs compatibles), y AMD 64 bits.



Referencia Web:
http://www.edubuntu.org/



Panda Software presenta mundialmente su iniciativa solidaria "Panda IT Aid" con ayudas de más de €100.000 en donativos.

Panda Software ha creado el programa de ayudas "Panda IT Aid" que apoyará con una donación económica de más de €100.000 a proyectos de solidaridad digital la idea es hacer realidad 15 proyectos de entidades sin fines de lucro que contribuyan al acceso universal e igualitario y a un uso seguro de las tecnologías de la información.

La ayuda económica total consiste en medio millón de euros: €100.000 en efectivo que se destinarán a los cuatro proyectos ganadores (25.000 euros a cada un de ellos) y hasta 400.000 euros en productos y servicios de seguridad informática de Panda Software, a repartir entre los 15 proyectos finalistas.

Un comité de representantes de la compañía, instituciones públicas y expertos externos en acción social, seleccionará los 15 proyectos finalistas, luego de lo cual votarán más de 50 filiales internacionales de Panda para elegir los cuatro proyectos que recibirán el gran premio. Los criterios a juzgar serán: creatividad, impacto social, y replicabilidad, entre otros.

El plazo para presentarse a esta iniciativa finaliza el próximo 24 de abril. Los proyectos deberán ser remitidos por correo electrónico a pandaITaid@pandasoftware.com. Realizar consultas en: *www.PandaITaid.es*





CeBIT HANNOVER 2006

Entre el 9 y el 15 de marzo en Hannover, Alemania, tuvo lugar la CeBIT, la convención más grande del mundo en su tipo, presentando soluciones de IT y telecomunicaciones para hogares y ambientes laborales. En su vigésimo aniversario, contó con una asistencia de 450.000 visitantes que superó por amplio margen a todos los registros de las anteriores ediciones; ésto satisfizo a los 6.262 expositores que firmaron varios contratos por millones de dólares, y cerrado un 20% más de tratados comerciales durante esta convención que en edición 2005. Se hizo notar el incremento del 30% en la presencia de pequeñas y medianas empresas (con no más de 500 empleados), que tuvieron su propio forum.
También tuvieron la oportunidad para ver las novedades del sector, los retailers, quienes junto con distribuidoras, corporaciones de compras, y cadenas minoristas para venta al consumidor final tuvieron un punto de encuentro común, el "Planet Reseller" una muestra de cómo la CeBIT intenta atraer a sectores específicos de la industria.
A lo largo y ancho de los 100.000 metros cuadrados del predio donde se desarrolló el evento, los temas en exposición estuvieron distribuidos en pasillos, uno de los cuales le correspondió al sector de tecnologías Bancarias y Financieras; un tema popular en éste fue la implementación de las redes a las ventas, control, y producción junto con la seguridad de las transacciones electrónicas. En el sector público, están siendo diseñadas interfaces basadas en estándares abiertos para promover procesos transparentes y simplificados.
- *http://www.cebit.de*

Humor - *Por Severi*

